

Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking **High**. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
 - ASP Knowledgebase SQL Injection Vulnerability
 - FileZilla Server Terminal Privilege Elevation or Arbitrary Code Execution
 - WhatsUp Small Business Directory Traversal and Information Disclosure
 - **Microsoft DirectX DirectShow Arbitrary Code Execution (Updated)**
 - **Microsoft Windows EMF File Denial of Service Vulnerability (Updated)**
 - Microsoft Windows Graphics Rendering Engine Arbitrary Code Execution
 - Microsoft Windows Kerberos PKINIT Information Disclosure or Denial of Service
 - Ocean12 Calendar Manager Pro Authentication Bypassing
- UNIX / Linux Operating Systems
 - **Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass (Updated)**
 - Asterisk Voicemail Unauthorized Access
 - Linux-FTPD-SSL FTP Server Remote Buffer Overflow
 - cPanel Cross-Site Scripting
 - Debian Horde Default Administrator Password
 - **eric3 Unspecified Vulnerability (Updated)**
 - **Elm 'Expires' Header Remote Buffer Overflow (Updated)**
 - **Eric Raymond Fetchmail 'fetchmailconf' Information Disclosure (Updated)**
 - F-Secure Anti-Virus Gatekeeper & Gateway for Linux Elevated Privileges
 - **Gallery PostNuke Access Validation (Updated)**
 - **Gentoo Linux Multiple Packages Insecure RUNPATH (Updated)**
 - GpsDrive Remote Format String
 - HP-UX ftpd LIST Command Information Disclosure
 - HP-UX 'envd' Arbitrary Code Execution or Elevated Privileges
 - HP-UX Trusted Mode 'remshd' Remote Unauthorized Access
 - IBM AIX SWCONS Local Buffer Overflow
 - **Jed Wing CHM Lib 'chm_find' in PMGL Remote Buffer Overflow (Updated)**
 - **Jed Wing CHM Lib Remote Buffer Overflow (Updated)**
 - **KDE KOffice KWord RTF Remote Buffer Overflow (Updated)**
 - **LM sensors PWMConfig Insecure Temporary File Creation (Updated)**
 - Clam AntiVirus Remote Denial of Service& Arbitrary Code Execution
 - **Multiple Vendors ht://Dig Cross-Site Scripting (Updated)**
 - Jed Wing CHM Lib LZX Decompression Method Buffer Overflow
 - Multiple Vendors Pax File Permission Modification Race Condition
 - **Multiple Vendors Squid NTLM Authentication Remote Denial of Service (Updated)**
 - **Zlib Compression Library Buffer Overflow (Updated)**
 - **Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service (Updated)**
 - Multiple Vendors Acme Thttpd Insecure Temporary File Creation
 - **Multiple Vendors GNOME-DB LibGDA Multiple Format String (Updated)**
 - **Multiple Vendors GNUMP3d Cross-Site Scripting or Directory Traversal (Updated)**
 - Multiple Vendors GNU gnump3d Unspecified Cross-Site Scripting
 - Multiple Vendors Linux Kernel 'Sysctl' Denial of Service
 - **Multiple Vendor WGet/Curl NTLM Username Buffer Overflow (Updated)**
 - **Multiple Vendors OpenSSL Insecure Protocol Negotiation (Updated)**
 - Multiple Vendors libungif GIF File Handling
 - **Multiple Vendors XNTPD Insecure Privileges (Updated)**
 - Multiple Vendors CHFN User Modification ROOT Access
 - Multiple Vendor 'ReadDir_R' Buffer Overflow
 - NetBSD Kernel, Networking & Application Code Denial of Service, Information Disclosure or Elevated Privileges
 - **OpenVPN Client Remote Format String & Denial of Service (Updated)**
 - **PHPMyAdmin Cross-Site Scripting (Updated)**
 - **phpMyAdmin Local File Inclusion & Cross-Site Scripting (Updated)**
 - **Squid Aborted Requests Remote Denial of Service (Updated)**
 - **Squid 'sslConnectTimeout()' Remote Denial of Service (Updated)**
 - **Squid FTP Server Response Handling Remote Denial of Service (Updated)**
 - Sylpheed LDIF Import Buffer Overflow
 - **Todd Miller Sudo Local Elevated Privileges (Updated)**
 - **UW-imapd Denial of Service and Arbitrary Code Execution (Updated)**
 - **up-imaproxy Format String (Updated)**

- VERITAS Cluster Server for UNIX Buffer Overflow
- [**Zope 'RestructuredText' Unspecified Security Vulnerability \(Updated\)**](#)
- [Multiple Operating Systems](#)
 - [**Apache HTTP Request Smuggling Vulnerability \(Updated\)**](#)
 - [Apache Tomcat Remote Denial of Service](#)
 - [Apple QuickTime Player Integer & Buffer Overflows](#)
 - [ATutor SQL Injection](#)
 - [Belchior Foundry vCard Pro SQL Injection](#)
 - [Cisco Airespace Wireless LAN Controller Unencrypted Connections](#)
 - [Cisco IOS System Timers Heap Buffer Overflow](#)
 - [**Cisco Management Center for IPS Sensors Signature Disable \(Updated\)**](#)
 - [CutePHP CuteNews Directory Traversal & PHP Code Execution](#)
 - [Elite Forum HTML Injection](#)
 - [F-Prot Antivirus ZIP Attachment Version Scan Bypass](#)
 - [F-Secure Web Console Directory Traversal](#)
 - [Gallery SQL Injection](#)
 - [IBM Lotus Domino/Notes Multiple Vulnerabilities](#)
 - [IBM Tivoli Directory Server Security Bypass](#)
 - [IBM WebSphere Application Server Information Disclosure](#)
 - [ibProArcade Module SQL Injection](#)
 - [Invision Power Board Multiple Cross-Site Scripting](#)
 - [Jelsoft Enterprises vBulletin Image Upload Input Validation](#)
 - [Johannes F. Kuhlmann FlatFrag Remote Buffer Overflow & Denial of Service](#)
 - [JPortal Multiple SQL Injection](#)
 - [Macromedia Flash Array Index Remote Arbitrary Code Execution](#)
 - [Macromedia Flash Input Validation](#)
 - [**Mozilla/Netscape/Firefox Browsers Domain Name Buffer Overflow \(updated\)**](#)
 - [**Ethereal Denial of Service \(Updated\)**](#)
 - [Multiple Vendor Web Browser Cookie Hostname Information Disclosure](#)
 - [**Multiple Vendors PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution \(Updated\)**](#)
 - [Multiple Vendors PunBB/Blog:CMS HTML Injection, Origin Spoof & Information Disclosure](#)
 - [Multiple Vendors PHP Group Exif Module Remote Denial of Service](#)
 - [**Multiple Vendors Ethereal Multiple Protocol Dissector Vulnerabilities \(Updated\)**](#)
 - [**Multiple Vendors Lynx 'HTriis\(\)' NNTP Remote Buffer Overflow \(Updated\)**](#)
 - [**Multiple Vendors XML-RPC for PHP Remote Code Injection \(Updated\)**](#)
 - [OSTE File Inclusion Vulnerability](#)
 - [PHP Handicapper Cross-Site Scripting & SQL Injection](#)
 - [**PHP Multiple Vulnerabilities \(Updated\)**](#)
 - [PHPBB Forum Cross-Site Scripting](#)
 - [PHPFM Arbitrary File Upload](#)
 - [PHPKit Multiple Input Validation](#)
 - [PHPList Multiple Input Validation](#)
 - [phpWebThings Cross-Site Scripting & SQL Injection](#)
 - [SAP Web Application Server HTTP Response Splitting, Cross-Site Scripting & URI Redirection](#)
 - [Scorched 3D Multiple Vulnerabilities](#)
 - [Six Apart Movable Type Arbitrary Blog Creation Path & Entry Posting HTML Injection](#)
 - [**SquirrelMail Variable Handling \(Updated\)**](#)
 - [Sun Java Development Kit Font Serialization Remote Denial of Service](#)
 - [XMB Cross-Site Scripting](#)
 - [XMB Forum SQL Injection](#)
 - [toendaCMS Information Disclosure](#)
 - [VERITAS NetBackup Volume Manager Daemon Buffer Overflow](#)
 - [VUBB Cross-Site Scripting & Path Disclosure](#)
 - [Web Group Media Cerberus Helpdesk Information Disclosure](#)
 - [YaBB Image Upload HTML Injection](#)

[Wireless](#)

[Recent Exploit Scripts/Techniques](#)

[Trends](#)

[Viruses/Trojans](#)

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the [Multiple Operating Systems](#) section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
ASP Knowledgebase	A vulnerability has been reported in ASPKnowledgebase that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	ASP Knowledgebase SQL Injection Vulnerability	Medium	Security Focus, ID: 15364, November 9, 2005
FileZilla Server Terminal 0.4.9d	A buffer overflow vulnerability has been reported in FileZilla that could let remote malicious users obtain elevated privileges or execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	FileZilla Server Terminal Privilege Elevation or Arbitrary Code Execution	High	Security Focus, ID: 15346, November 7, 2005
IpSwitch WhatsUp Small Business 2004	An input validation vulnerability has been reported in WhatsUp Small Business that could let remote malicious users to traverse directories and disclose information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	WhatsUp Small Business Directory Traversal and Information Disclosure CVE-2005-1939	Medium	Security Tracker, Alert ID: 1015141, November 3, 2005
Microsoft DirectX DirectShow 7.0 to 9.0c	A buffer overflow vulnerability has been reported in DirectX DirectShow that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf V1.3 Updated to note availability of Microsoft Knowledge Base Article 909596 and to clarify an issue affecting Windows 2000 SP4 customers, also updates of file versions. V1.4 Updated to note complications of the DirectX 8.1 update on machines running DirectX 9. Currently we are not aware of any exploits for this vulnerability.	Microsoft DirectX DirectShow Arbitrary Code Execution CVE-2005-2128	High	Microsoft, Security Bulletin MS05-050, October 11, 2005 USCERT, VU#995220 Technical Cyber Security Alert TA05-284A, October 11, 2005 Avaya, ASA-2005-214, October 11, 2005 Microsoft, Security Bulletin MS05-050 V1.3, October 21, 2005 Microsoft, Security Bulletin MS05-050 V1.4, November 9, 2005
Microsoft Microsoft Windows 2000 Advanced Server Microsoft Windows 2000 Datacenter Server Microsoft Windows 2000 Professional Microsoft Windows 2000 Server	A vulnerability has been reported that could let remote malicious users cause a Denial of Service. This is due to an error when processing EMF (Microsoft Enhanced Metafile) files in the 'GetEnhMetaFilePaletteEntries()' API in 'GDI32.DLL.' Vendor solution available: http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx Proof of Concept exploits have been published.	Microsoft Windows EMF File Denial of Service Vulnerability CVE-2005-0803	Low	Secunia SA14631, March 18, 2005 Security Focus, ID: 12834, November 9, 2005 Microsoft, Security Bulletin MS05-053, November 8, 2005 US-CERT, VU#134756, November 9, 2005
Microsoft Windows Graphics Rendering Engine	A buffer overflow vulnerability has been reported in Windows Graphics Rendering Engine that could let local or remote malicious users execute arbitrary code. Vendor solution available:	Microsoft Windows Graphics Rendering Engine Arbitrary Code Execution	High	Security Tracker, Alert ID: 1015168, November 8, 2005 Microsoft, Security

	http://www.microsoft.com/technet/security/Bulletin/MS05-053.msp Currently we are not aware of any exploits for this vulnerability.	CVE-2005-2123 CVE-2005-2124	Bulletin MS05-053, November 8, 2005 US-CERT, VU#433341 , VU#300549 , November 9, 2005
Microsoft Windows Kerberos PKINT	Multiple vulnerabilities have been reported in Windows Kerberos PKINT that could let remote malicious users disclose information or cause a Denial of Service. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-042.msp Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Kerberos PKINIT Information Disclosure or Denial of Service CAN-2005-1981 CAN-2005-1982	Low Microsoft Security Bulletin MS05-042, August 9, 2005 US-CERT, VU#477341, November 9, 2005
Ocean12 Technologies Calendar Manager Pro 1.0, 1.0.1	A vulnerability has been reported in Calendar Manager Pro that could let remote malicious users to bypass authentication. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Ocean12 Calendar Manager Pro Authentication Bypassing	Medium Security Focus, ID: 15329, November 4, 2005

[back to top](#)

UNIX / Linux Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source

Apache Software Foundation	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyClient optional' directive, which could let a remote malicious user bypass security policies.	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CVE-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 Slackware Security Advisory, SSA:2005-251-02, September 9, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 Debian Security Advisory DSA 807-1, September 12, 2005 US-CERT VU#744929 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Avaya Security Advisory, ASA-2005-204, September 23, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005 HP Security Bulletin, HPSBUX-01232, October 5, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 RedHat Security Advisory, RHSA-2005:816-10, November 2, 2005
Apache 2.0.x	<p>Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/</p> <p>SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/</p> <p>Debian: http://security.debian.org/pool/updates/main/a/apache2/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Debian: http://security.debian.org/pool/updates/main/liba/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200509-12.xml</p> <p>Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</p> <p>HP: http://software.hp.com/</p>			

	<p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-816.html</p> <p>There is no exploit code required.</p>			
<p>Asterisk</p> <p>Asterisk@Home 2.0-beta4, 1.5, Asterisk 1.2.0-beta1, 1.0.9, 1.0.8, 1.0.7, 0.9.0, 0.7-0.7.2, 0.4, 0.3, 0.2, 0.1.7-0.1.9-1</p>	<p>A vulnerability has been reported in 'vmail.cgi' due to insufficient sanitization of the 'folder' parameter, which could let a remote malicious user obtain unauthorized access.</p> <p>Upgrades available at: http://ftp.digium.com/pub/asterisk/asterisk-1.2.0-beta2.tar.gz</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>Asterisk Voicemail Unauthorized Access</p>	<p>Medium</p>	<p>Assurance.com.au Vulnerability Advisory, November 7, 2005</p>
<p>Christoph Martin</p> <p>linux-ftpd-ssl 0.17</p>	<p>A buffer overflow vulnerability has been reported in the 'vsprintf()' function in the FTP server, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>An exploit script has been published.</p>	<p>Linux-FTPD-SSL FTP Server Remote Buffer Overflow</p> <p>CVE-2005-3524</p>	<p>High</p>	<p>Secunia Advisory: SA17465, November 8, 2005</p>
<p>cPanel Inc.</p> <p>cPanel 10.6.0-R137, 10.2.0-R82</p>	<p>A Cross-Site Scripting vulnerability has been reported in the Entropy Chat script due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>cPanel Cross-Site Scripting</p> <p>CVE-2005-3505</p>	<p>Medium</p>	<p>Secunia Advisory: SA16609, November 4, 2005</p>
<p>Debian</p> <p>horde 3.0.4</p>	<p>A vulnerability has been reported because the default Horde3 installation for Debian has a blank administrator password, which could let a local/remote malicious user obtain administrative access.</p> <p>Upgrade available at: http://security.debian.org/pool/updates/main/h/horde3/horde3_3.0.4-4sarge1_all.deb</p> <p>There is no exploit code required.</p>	<p>Debian Horde Default Administrator Password</p> <p>CVE-2005-3344</p>	<p>High</p>	<p>Debian Security Advisory, DSA 884-1, November 7, 2005</p>
<p>Detlev Offenbach</p> <p>eric3 prior to 3.7.2</p>	<p>A vulnerability has been reported due to a "potential security exploit." The impact was not specified</p>	<p>eric3 Unspecified Vulnerability</p>	<p>Not Specified</p>	<p>Security Tracker Alert ID: 1014947, September 21, 2005</p> <p>Debian Security</p>

	<p>Upgrades available at: http://prdownloads.sourceforge.net/eric-ide/eric-3.7.2.tar.gz?download</p> <p>Debian: http://security.debian.org/pool/updates/main/e/eric/</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	CVE-2005-3068		<p>Advisory, DSA 869-1, October 21, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p>
<p>Elm Development Group</p> <p>ELM 2.5.5-2.5.7</p>	<p>A buffer overflow vulnerability has been reported due to insufficient parsing of SMTP 'Expires' header lines, which could let a remote malicious user execute arbitrary code.</p> <p>Update to Elm 2.5 PL8 available at: ftp://ftp.virginia.edu/pub/elm/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-755.html</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>A Proof of Concept exploit script has been published.</p>	<p>Elm 'Expires' Header Remote Buffer Overflow</p> <p>CVE-2005-2665</p>	High	<p>Security Tracker Alert ID: 1014745, August 20, 2005</p> <p>RedHat Security Advisory, RHSA-2005:755-07, August 23, 2005</p> <p>Slackware Security Advisory, SSA:2005-311-01, November 8, 2005</p>
<p>Eric S Raymond</p> <p>Fetchmail 6.x</p>	<p>A vulnerability has been reported in the 'fetchmailconf' configuration utility due to a race condition, which could let a malicious user obtain sensitive information.</p> <p>Upgrades available at: http://download.berlios.de/fetchmail/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200511-06.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/f/fetchmail/</p> <p>There is no exploit code required.</p>	<p>Fetchmail 'fetchmailconf' Information Disclosure</p> <p>CVE-2005-3088</p>	Medium	<p>fetchmail-SA-2005-02 Security Announcement, October 21, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200511-06, November 6, 2005</p> <p>Ubuntu Security Notice, USN-215-1, November 07, 2005</p>
<p>F-Secure</p> <p>Internet Gatekeeper for Linux, Anti-Virus for Linux Gateways</p>	<p>A vulnerability has been reported because certain CGI scripts that have world-executable permissions and set user id (setuid) permissions can be invoked by a malicious user to obtain root privileges.</p> <p>Fix available at: http://www.f-secure.co.jp/download/</p> <p>There is no exploit code required; however, a Proof of Concept exploit script has been published.</p>	<p>F-Secure Anti-Virus Gatekeeper & Gateway for Linux Elevated Privileges</p>	High	<p>F-Secure Security Bulletin FSC-2005-3, November 7, 2005</p>

Gallery Gallery 1.5 1.4 -1.4.4 -pl5	<p>A vulnerability has been reported in 'classes/postnuke0.7.1/user.php' when determining the gallery name due to incorrect use of the global '\$name' variable, which could let a remote malicious user bypass security restrictions.</p> <p>Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=7130&package_id=7239&release_id=348064</p> <p>Debian: http://security.debian.org/pool/updates/main/g/gallery/</p> <p>There is no exploit code required.</p>	<p>Gallery PostNuke Access Validation</p> <p>CVE-2005-2596</p>	Medium	<p>Secunia Advisory: SA16389, August 11, 2005</p> <p>Debian Security Advisory, DSA 879-1, November 2, 2005</p>
Gentoo Linux Gentoo Linux	<p>Vulnerabilities have been reported in multiple packages in Gentoo Linux due to an insecure RUNPATH vulnerability, which could let a malicious user obtain elevated privileges.</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200510-14.xml</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200511-02.xml</p> <p>There is no exploit code required.</p>	<p>Gentoo Linux Multiple Packages Insecure RUNPATH</p>	Medium	<p>Gentoo Linux Security Advisory, GLSA 200510-14, October 17, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200511-02, November 2, 2005</p>
GpsDrive GpsDrive 2.0 9	<p>A format string vulnerability has been reported in 'Friendsd,' which could let a remote malicious user execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/main/g/gpsdrive/</p> <p>Proof of Concept exploits have been published.</p>	<p>GpsDrive Remote Format String</p> <p>CVE-2005-3523</p>	High	<p>Security Focus, Bugtraq ID: 15319, November 4, 2005</p> <p>Debian Security Advisory, DSA 891-1, November 9, 2005</p>
Hewlett Packard Company HP-UX 11.0 4, 11.0, 10.20, B.11.11, B.11.04, B.11.00	<p>A vulnerability was reported because remote malicious authenticated users can send specially crafted data to list directories with root privileges.</p> <p>Updates available at: http://itrc.hp.com</p> <p>There is no exploit code required; however, a Proof of Concept exploit script has been published.</p>	<p>HP-UX ftpd LIST Command Information Disclosure</p> <p>CVE-2005-3296</p>	Medium	<p>HP Security Advisory, HPSBUX 02071, November 6, 2005</p>
Hewlett Packard Company HP-UX B.11.00, B.11.11	<p>A vulnerability has been reported in 'envd' due to an unspecified error, which could let a remote malicious user execute arbitrary code and/or obtain elevated privileges.</p> <p>Patches available at: http://itrc.hp.com</p> <p>Currently we are not aware</p>	<p>HP-UX 'envd' Arbitrary Code Execution or Elevated Privileges</p>	High	<p>HP Security Bulletin, HPSBUX 02073, November 9, 2005</p>

	of any exploits for this vulnerability.			
Hewlett Packard Company HP-UX B.11.00, B.11.11, B.11.23	A vulnerability has been reported in 'remshd' due to an unspecified error on systems running in Trusted Mode, which could let a remote malicious user obtain unauthorized access. Patches available at: http://itrc.hp.com Currently we are not aware of any exploits for this vulnerability.	HP-UX Trusted Mode 'remshd' Remote Unauthorized Access	Medium	HP Security Bulletin, HPSBUX 02072, November 9, 2005
IBM AIX 5.2.2, 5.2L, 5.2	A buffer overflow vulnerability has been reported in 'SWCONS' command due to a boundary error. The impact was not specified. Update information available at: http://www-1.ibm.com/support/docview.wss?uid=isg1IY78467 Currently we are not aware of any exploits for this vulnerability.	IBM AIX SWCONS Local Buffer Overflow CVE-2005-3504	Not Specified	IBM Advisory, IY78467, November 3, 2005
Jed Wing CHM lib 0.35, 0.3- 0.33, 0.2, 0.1	A buffer overflow vulnerability has been reported in '_chm_find_in_PMG'L' due to a failure to properly bounds check input data prior to copying it into an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.36.tgz Debian: http://security.debian.org/pool/updates/main/c/chmlib/ Currently we are not aware of any exploits for this vulnerability.	Jed Wing CHM Lib '_chm_find_in_PMG'L Remote Buffer Overflow CVE-2005-2930	High	iDefense Security Advisory, October 28, 2005 Debian Security Advisory, DSA 886-1, November 7, 2005
Jed Wing CHM lib 0.36, 0.35, 0.3-0.33, 0.2, 0.1	A buffer overflow vulnerability has been reported in the '_chm_decompress_block()' function due to a boundary error when reading input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.37.tgz SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/c/chmlib/ Currently we are not aware of any exploits for this vulnerability.	CHM Lib Remote Buffer Overflow CVE-2005-3318	High	Security Focus, Bugtraq ID: 15211, October 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Debian Security Advisory, DSA 886-1, November 7, 2005

<p>KDE</p> <p>KOffice 1.4.1, 1.4, 1.3-1.3.5, 1.2.1, 1.2</p>	<p>A buffer overflow vulnerability has been reported when handling a malformed RTF file, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrades available at: http://www.koffice.org/download/</p> <p>Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/k/koffice/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200510-12.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/k/koffice/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Debian: http://security.debian.org/pool/updates/main/k/koffice/</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>KDE KOffice KWord RTF Remote Buffer Overflow</p> <p>CVE-2005-2971</p>	<p>High</p>	<p>Security Focus, Bugtraq ID: 15060, October 11, 2005</p> <p>Ubuntu Security Notice, USN-202-1, October 12, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200510-12, October 12, 2005</p> <p>Fedora Update Notification, FEDORA-2005-984, October 13, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:185, October 14, 2005</p> <p>Debian Security Advisory, DSA 872-1, October 26, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p> <p>Slackware Security Advisory, SSA:2005-310-02, November 7, 2005</p> <p>Conectiva Security Announce-ment, CLSA-2005:1042, November 7, 2005</p>
<p>Im_sensors</p> <p>Im_sensors 2.9.1</p>	<p>A vulnerability has been reported in the 'pwmconfig' script due to the insecure creation of temporary files, which could result in a loss of data or a Denial of Service.</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lm-sensors/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200508-19.xml</p> <p>Debian:</p>	<p>LM_sensors PWMConfig Insecure Temporary File Creation</p> <p>CVE-2005-2672</p>	<p>Low</p>	<p>Security Focus, Bugtraq ID: 14624, August 22, 2005</p> <p>Ubuntu Security Notice, USN-172-1, August 23, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:149, August 25, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200508-19, August 30, 2005</p> <p>Debian Security Advisory, DSA 814-1, September 15, 2005</p> <p>Conectiva Linux Announce-ment, CLSA-2005:1012,</p>

	http://security.debian.org/pool/updates/main/lm-sensors/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ There is no exploit code required.			September 23, 2005 Fedora Update Notifications, FEDORA-2005-1053 & 1054, November 7, 2005
Multiple Vendors ClamAV 0.80-0.87, 0.75.1, 0.70, 0.68, 0.65, 0.60, 0.51-0.54	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'libclamav/fsg.c' due to a boundary error when unpacking FSG v1.33 compressed executable files, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in 'libclamav/tnef.c' due to a validation error when handling a CAB file that contains a malformed header; a remote Denial of Service vulnerability was reported in 'libclamav/mspack/cabd.c' due to an error when handling a CAB file that contains a malformed header; and a remote Denial of Service vulnerability was reported in 'libclamav/ole2_extract.c' because the OLE2 unpacker does not properly process DOC files with an invalid property tree. Upgrades available at: http://prdownloads.sourceforge.net/clamav/clamav-0.87.1.tar.gz?download Debian: http://security.debian.org/pool/updates/main/c/clamav/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-04.xml Mandriva: http://www.mandriva.com/security/advisories Currently we are not aware of any exploits for these vulnerabilities.	Clam AntiVirus Remote Denial of Service & Arbitrary Code Execution CVE-2005-3303 CVE-2005-3239 CVE-2005-3500 CVE-2005-3501	High	Security Tracker Alert ID: 1015154, November 4, 2005 Debian Security Advisory DSA 887-1, November 7, 2005 Gentoo Linux Security Advisory, GLSA 200511-04, November 7, 2005 Mandriva Linux Security Advisory, MDKSA-2005:205, November 7, 2005
Multiple Vendors ht://Dig Group ht://Dig 3.1.5 -8, 3.1.5 -7, 3.1.5, 3.1.6, 3.2 .0, 3.2 0b2-0b6; SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, 9.0 x86_64, 9.1, 9.2	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from the 'config' parameter, which could let a remote malicious user execute arbitrary HTML and script code. SuSE: ftp://ftp.suse.com/pub/suse/ Debian:	ht://Dig Cross-Site Scripting CVE-2005-0085	High	SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Debian Security Advisory, DSA 680-1, February 14, 2005 Gentoo Linux Security Advisory, GLSA 200502-16, February 14, 2005

	http://security.debian.org/pool/updates/main/h/htdig/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SCO: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.46/507 Proof of Concept exploit has been published.			Mandrakelinux Security Update Advisory, MDKSA-2005:063, March 31, 2005 Fedora Update Notification, FEDORA-2005-367, April 19, 2005 SCO Security Advisory, SCOSA-2005.46, November 2, 2005
Multiple Vendors Jed Wing CHM lib 0.35-0.37, 0.3-0.33, 0.2, 0.1; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A buffer overflow vulnerability has been reported in the LZX decompression method, which could possibly let a remote malicious user execute arbitrary code. Upgrade available at: http://morte.jedrea.com/~jedwin/projects/chmlib/chmlib-0.37.4.tgz Debian: http://security.debian.org/pool/updates/main/c/chmlib/ Currently we are not aware of any exploits for this vulnerability.	Jed Wing CHM Lib LZX Decompression Method Buffer Overflow CVE-2005-2659	High	Debian Security Advisory DSA 886-1, November 7, 2005
Multiple Vendors OpenBSD 3.0-3.7, 2.0-2.9; Keith Muller pax	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. OpenBSD: http://www.openbsd.org/38.html There is no exploit code required;	Pax File Permission Modification Race Condition	Medium	Security Focus, Bugtraq ID: 15262, November 1, 2005
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE3-STABLE10, STABLE1	A remote Denial of Service vulnerability has been reported when handling certain client NTLM authentication request sequences. Upgrades available at: http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE11.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Debian: http://security.debian.org/pool/updates/main/s/squid/	Squid NTLM Authentication Remote Denial of Service CVE-2005-2917	Low	Secunia Advisory: SA16992, September 30, 2005 Ubuntu Security Notice, USN-192-1, September 30, 2005 Debian Security Advisory, DSA 828-1, September 30, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:181, October 11, 2005 SCO Security Advisory, SCOSA-2005.44, November 1, 2005

	<p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.44</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			<p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p>
<p>Multiple Vendors</p> <p>zlib 1.2.2, 1.2.1, 1.2.0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELEASE, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELEASE, -RELEASE;</p> <p>Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3, 0.1-0.1.6 1, 0.0.1-0.0.6</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>OpenBSD: http://www.openbsd.org/errata.html</p> <p>OpenPKG: ftp.openpkg.org</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/</p>	<p>A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code.</p> <p>Debian: ftp://security.debian.org/pool/updates/main/z/zlib/</p> <p>FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>OpenBSD: http://www.openbsd.org/errata.html</p> <p>OpenPKG: ftp.openpkg.org</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/</p>	<p>Zlib Compression Library Buffer Overflow</p> <p>CVE-2005-2096</p>	<p>High</p>	<p>Debian Security Advisory DSA 740-1, July 6, 2005</p> <p>FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005</p> <p>Ubuntu Security Notice, USN-148-1, July 06, 2005</p> <p>RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0034, July 8, 2005</p> <p>Slackware Security Advisory, SSA:2005-189-01, July 11, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005</p> <p>Fedora Update Notification, FEDORA-2005-565, July 13, 2005</p> <p>SUSE Security Summary Report,</p>

linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id=35093&release_id=351848 Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trolltech: ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz FedoraLegacy: http://download.fedoralegacy.org/fedora/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-18.xml Gentoo: http://security.gentoo.org/glsa/glsa-200509-18.xml Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trustix: http://http.trustix.org/pub/trustix/updates/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101989-1 Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/aide/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/r/rpm/ <p>Currently we are not aware of any exploits for this vulnerability.</p>	SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14162, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 Gentoo Linux Security Advisory, GLSA 200509-18, September 26, 2005 Debian Security Advisory, DSA 797-2, September 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005 Sun(sm) Alert Notification Sun Alert ID: 101989, October 14, 2005 Mandriva Linux Security Advisory MDKSA-2005:196, October 26, 2005 Ubuntu Security Notice, USN-151-3, October 28, 2005 Ubuntu Security Notice, USN-151-4, November 09, 2005
--	---

Multiple Vendors	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input.	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CVE-2005-1849	Low	Security Focus, Bugtraq ID 14340, July 21, 2005
zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	<p>Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz</p> <p>Debian: http://security.debian.org/pool/updates/main/z/zlib/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/</p> <p>OpenBSD: http://www.openbsd.org/errata.html#libz2</p> <p>Mandriva: http://www.mandriva.com/security/advisories?name=MDKSA-2005:124</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596</p> <p>FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc</p> <p>SUSE: http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200507-28.xml</p> <p>http://security.gentoo.org/glsa/glsa-200508-01.xml</p> <p>Trustix: ftp://ftp.trustix.org/pub/trustix/updates/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>Apple: http://docs.info.apple.com/article.html?artnum=302163</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/</p> <p>SCO: ftp://ftp.sco.com/pub/updates/UnixWare/</p>			<p>Debian Security Advisory DSA 763-1, July 21, 2005</p> <p>Ubuntu Security Notice, USN-151-1, July 21, 2005</p> <p>OpenBSD, Release Errata 3.7, July 21, 2005</p> <p>Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005</p> <p>Secunia, Advisory: SA16195, July 25, 2005</p> <p>Slackware Security Advisory, SSA:2005-203-03, July 22, 2005</p> <p>FreeBSD Security Advisory, SA-05:18, July 27, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0040, August 5, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005</p> <p>Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-83, August 18, 2005</p> <p>SCO Security Advisory, SCOSA-2005.33, August 19, 2005</p> <p>Debian Security Advisory, DSA 797-1, September 1, 2005</p> <p>Security Focus, Bugtraq ID: 14340, September 12, 2005</p> <p>Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005</p> <p>Debian Security Advisory, DSA 797-2, September 29, 2005</p> <p>Mandriva Linux Security Advisory,</p>

	<p>SCOSA-2005.33</p> <p>Debian: http://security.debian.org/pool/updates/main/z/zsync/</p> <p>Trolltech: ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz</p> <p>FedoraLegacy: http://download.fedoralegacy.org/fedora/</p> <p>Debian: http://security.debian.org/pool/updates/main/z/zsync/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/aide/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/r/rpm/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			<p>MDKSA-2005:196, October 26, 2005</p> <p>Ubuntu Security Notice, USN-151-3, October 28, 2005</p> <p>Ubuntu Security Notice, USN-151-4, November 09, 2005</p>
Multiple Vendors	<p>A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user overwrite arbitrary files.</p> <p>Debian: http://security.debian.org/pool/updates/main/t/thttpd/</p> <p>There is no exploit code required.</p>	<p>Acme Thttpd Insecure Temporary File Creation</p> <p>CVE-2005-3124</p>	Medium	<p>Debian Security Advisory DSA 883-1, November 4, 2005</p>
<p>Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Acme thttpd 2.23 b1, 2.21 b</p>				
Multiple Vendors	<p>Format string vulnerabilities have been reported in 'gda-log.c' due to format string errors in the 'gda_log_error()' and 'gda_log_message()' functions, which could let a remote malicious user execute arbitrary code.</p> <p>Debian: http://security.debian.org/pool/updates/main/libg/libgda2/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgda2/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200511-01.xml</p> <p>SUSE: ftp://ftp.suse.com</p>	<p>GNOME-DB LibGDA Multiple Format String</p> <p>CVE-2005-2958</p>	High	<p>Security Focus, Bugtraq ID: 15200, October 25, 2005</p> <p>Debian Security Advisory, DSA-871-1 & 871-2, October 25, 2005</p> <p>Ubuntu Security Notice, USN-212-1, October 28, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:203, November 1, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200511-01, November 2, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p> <p>Fedora Update Notification, FEDORA-2005-1029, November 7, 2005</p>
<p>Gnome-DB libgda 1.2.1; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha</p>				

	/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors GNU gnutmp3d 2.9-2.9.5; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in GNUMP3d that could let remote malicious users conduct Cross-Site Scripting or traverse directories. Upgrade to version 2.9.6: http://savannah.gnu.org/download/gnutmp3d/gnutmp3d-2.9.6.tar.gz Debian: http://security.debian.org/pool/updates/main/g/gnutmp3d/ SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-05.xml There is no exploit code required; however, Proof of Concept exploits have been published.	GNUMP3d Cross-Site Scripting or Directory Traversal CVE-2005-3122 CVE-2005-3123	Medium	Security Focus Bugtraq IDs: 15226 & 15228, October 28, 2005 Debian Security Advisory DSA 877-1, October 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Gentoo Linux Security Advisory, GLSA 200511-05, November 6, 2005
Multiple Vendors GNU gnutmp3d 2.9-2.9.5; Gentoo Linux	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.gnu.org/software/gnutmp3d/download.html#Download Gentoo: http://security.gentoo.org/glsa/glsa-200511-05.xml There is no exploit code required.	GNU gnutmp3d Unspecified Cross-Site Scripting CVE-2005-3425	Medium	Gentoo Linux Security Advisory GLSA 200511-05, November 7, 2005
Multiple Vendors Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been in 'sysctl.c' due to an error when handling the un-registration of interfaces in '/proc/sys/net/ipv4/conf/.' Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.1.tar.bz2 There is no exploit code required.	Linux Kernel 'Sysctl' Denial of Service CVE-2005-2709	Low	Secunia Advisory: SA17504, November 9, 2005
Multiple Vendors MandrakeSoft Multi Network Firewall 2.0, Linux Mandrake 2006.0 x86_64, 2006.0, 10.2	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied NTLM user name data, which could let a remote	Multiple Vendor WGet/Curl NTLM Username Buffer Overflow	High	Security Tracker Alert ID: 1015056, October 13, 2005 Mandriva Linux Security Update Advisories,

x86_64, 10.2, Corporate Server 3.0 x86_64, 3.0; GNU wget 1.10; Daniel Stenberg curl 7.14.1, 7.13.1, 7.13, 7.12.1- 7.12.3, 7.11- 7.11.2, 7.10.6- 7.10.8	<p>malicious user execute arbitrary code.</p> <p>WGet: http://ftp.gnu.org/pub/gnu/wget/wget-1.10.2.tar.gz</p> <p>Daniel Stenberg: http://curl.haxx.se/libcurl-ntlmbuf.patch</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200510-19.xml</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-807.html http://rhn.redhat.com/errata/RHSA-2005-812.html</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	CVE-2005-3185	MDKSA-2005:182 & 183, October 13, 2005 Ubuntu Security Notice, USN-205-1, October 14, 2005 Fedora Update Notifications FEDORA-2005-995 & 996, October 17, 2005 Fedora Update Notification, FEDORA-2005-1000, October 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 Gentoo Linux Security Advisory. GLSA 200510-19, October 22, 2005 RedHat Security Advisories, RHSA-2005:807-6 & RHSA-2005:812-5, November 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Slackware Security Advisory, SSA:2005-310-01, November 7, 2005
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, 2.1, IA64, ES 4, ES 3, 2.1, IA64, AS 4, AS 3, AS 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; OpenSSL Project OpenSSL 0.9.3-0.9.8, 0.9.2 b, 0.9.1 c; FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELEASE, -RELEASE, 5.3 -STABLE, -RELEASE, -RELEASE, 5.3, 5.2.1 -RELEASE, -RELEASE, 5.2 -RELEASE, 5.2, 5.1 -RELEASE, -RELEASE, -RELEASE/Alpha, 5.1 -RELEASE-p5, -RELEASE, 5.1, 5.0 -RELEASE, 5.0, 4.11 -STABLE, -RELEASE, 4.10 -RELEASE, -RELEASE, 4.10	<p>A vulnerability has been reported due to the implementation of the 'SSL_OP_MSIE_SSLV2_RSA_PADDING' option that maintains compatibility with third party software, which could let a remote malicious user bypass security.</p> <p>OpenSSL: http://www.openssl.org/source/openssl-0.9.7h.tar.gz</p> <p>FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:21/openssl.patch</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-800.html</p> <p>Mandriva: http://www.mandriva.com</p>	Multiple Vendors OpenSSL Insecure Protocol Negotiation CVE-2005-2969	Medium OpenSSL Security Advisory, October 11, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:21, October 11, 2005 RedHat Security Advisory, RHSA-2005:800-8, October 11, 2005 Mandriva Security Advisory, MDKSA-2005:179, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-11, October 12, 2005 Slackware Security Advisory, SSA:2005-286-01, October 13, 2005 Fedora Update

com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200510-11.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101974-1 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/openssl/ OpenPKG: ftp://ftp.openpkg.org/release/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: http://www.sgi.com/support/security/ Debian: http://security.debian.org/pool/updates/main/o/openssl094/ NetBSD: http://arkiv.netbsd.se/?ml=netbsd-announce&a=2005-10&m=1435804 BlueCoat Systems: http://www.bluecoat.com/support/knowledge/advisory_openssl_can-2005-2969.html Debian: http://security.debian.org/pool/updates/main/o/openssl/ Currently we are not aware of any exploits for this vulnerability.			Notifications, FEDORA-2005-985 & 986, October 13, 2005 Sun(sm) Alert Notification Sun Alert ID: 101974, October 14, 2005 Ubuntu Security Notice, USN-204-1, October 14, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.022, October 17, 2005 SUSE Security Announcement, SUSE-SA:2005:061, October 19, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 Debian Security Advisory DSA 875-1, October 27, 2005 NetBSD Security Update, November 1, 2005 BlueCoat Systems Advisory, November 3, 2005 Debian Security Advisory, DSA 888-1, November 7, 2005
--	--	--	--

Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, WS 2.1, IA64, ES 4, ES 3, ES 2.1, IA64, AS 4, AS 3, 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; libungif libungif 4.1.3, 4.1, giflib 4.1.3; Gentoo Linux	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported due to a NULL pointer dereferencing error; and a vulnerability was reported due to a boundary error that causes an out-of-bounds memory access, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary	Multiple Vendors libungif GIF File Handling CVE-2005-2974 CVE-2005-3350	High	Security Tracker Alert ID: 1015149, November 3, 2005 Fedora Update Notifications, FEDORA-2005-1045 & 1046, November 3, 2005 Gentoo Linux Security Advisory GLSA 200511-03, November 4, 2005 RedHat Security
---	---	--	------	---

	<p>code.</p> <p>Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=102202</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200511-03.xml</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-828.html</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libu/libungif4/</p> <p>Debian: http://security.debian.org/pool/updates/main/libu/libungif4/</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>			<p>code. Advisory, RHSA-2005:828-17, November 3, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p> <p>Ubuntu Security Notice, USN-214-1, November 07, 2005</p> <p>Debian Security Advisory, DSA 890-1, November 9, 2005</p>
<p>Multiple Vendors</p> <p>RedHat Fedora Core3; Ubuntu Linux 4.1 ppc, ia64, ia32; NTP NTPd 4.0-4.2 .0a</p>	<p>A vulnerability has been reported in xntpd when started using the '-u' option and the group is specified by a string, which could let a malicious user obtain elevated privileges.</p> <p>Upgrade available at: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/i386/ntp-4.2.0.a.20040617-5.FC3.i386.rpm</p> <p>NTP: http://ntp.isc.org/Main/DownloadViaHTTP?file=ntp4/snapshots/ntp-dev/20_05/08/ntp-dev-4.2.0b-20050827.tar.gz</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/n/ntp/</p> <p>Debian: http://security.debian.org/pool/updates/main/n/ntp/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>NetBSD: ftp://ftp.NetBSD.org/pub/NetBSD/</p>	<p>XNTPD Insecure Privileges</p> <p>CVE-2005-2496</p>	<p>Medium</p>	<p>Fedora Update Notification, FEDORA-2005-812, August 26, 2005</p> <p>Ubuntu Security Notice, USN-175-1, September 01, 2005</p> <p>Debian Security Advisory, DSA 801-1, September 5, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:156, September 6, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:1029, October 11, 2005</p> <p>NetBSD Security Advisory 2005-011, November 2, 2005</p>

[security/advisories/NetBSD-SA2005-011.txt.asc](#)

There is no exploit code required.

Multiple Vendors shadow shadow 4.0.3; Salvatore Valente chfn; SuSE UnitedLinux 1.0, Linux Professional 10.0 OSS, 10.0, 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64, Linux Personal 10.0 OSS, 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64, Linux Enterprise Server for S/390 9.0, 9, 8, Linux Desktop 1.0; pwdutils pwdutils 3.0.4, 2.6.96, 2.6.90, 2.6.4	A vulnerability has been reported in the setuid 'chfn' program due to insufficient argument checking when changing the GECOS field, which could let a malicious user obtain ROOT access. SUSE: ftp://ftp.suse.com/pub/suse/ An exploit script has been published.	Multiple Vendors CHFN User Modification ROOT Access CVE-2005-3503	High	SUSE Security Announcement, SUSE-SA:2005:064, November 4, 2005
Multiple Vendors XMail 1.21, 1.0; W3C Libwww 5.3.2, 3.1, 4.x; teTeX 2.0-2.0.2, 1.0.6, 1.0.7; TCL/TK 8.5 a2, 8.4.3, 8.4.2; SAOImage DS9 SAOImage DS9; Roxen WebServer 4.0.402, 2.2, 2.1.164, 2.1, 2.0.92, 2.0.69, 2.0 .X, 2.0, 1.4 .X, 1.3.122, 1.3 .X, 1.2 .X, 1.1 .X, 4.x, 3.x; Pike 7.7 .x, 7.6 .x, 7.4.327, 7.4 .x, 7.2 .x, 7.0 .x, 0.6 .x, 0.5 .x, 0.4 pl8; Peter Hofmann xgsmllib; OpenOffice OpenOffice 1.1.3; NETW netwib 5.30 .0, 5.1 .0; NcFTP Software NcFTP 3.1.9, 3.1.8; Mike Heffner BFBTester 2.0.1, 2.0; KDE 3.3-3.3.2; GNU gjc; firstworks Rudiments Library 0.28.2, 0.27; Bernhard R. Link reprepro	A buffer overflow vulnerability has been reported in certain uses of the 'readdir_r' function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor 'ReadDir_R' Buffer Overflow	High	Security Focus, Bugtraq ID: 15259, November 1, 2005
NetBSD NetBSD 2.0.2 & prior	Several vulnerabilities have been reported that could lead to a Denial of Service, sensitive information disclosure, or unauthorized access: a vulnerability was reported because the IPsec-AH calculation is always based on the same key in AES-XCBC-MAC; a vulnerability was reported because a malicious user can specify negative offsets when reading the message buffer to read arbitrary kernel memory; a vulnerability was reported in the 'imake(1)' function due to the insecure creation of temporary files; and a vulnerability was reported in the 'sh(1)' command. Update information available at: http://www.NetBSD .	NetBSD Kernel, Networking & Application Code Denial of Service, Information Disclosure or Elevated Privileges	Medium	Security Tracker Alert ID: 1015132, November 1, 2005

	org/mirrors/			There is no exploit code required.
OpenVPN OpenVPN 2.0-2.0.2	<p>Several vulnerabilities have been reported: a format string vulnerability was reported in 'options.c' when handling command options in the 'foreign_option()' function, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to a NULL pointer dereferencing error in the OpenVPN server when running in TCP mode.</p> <p>Updates available at: http://openvpn.net/download.html</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Debian: http://security.debian.org/pool/updates/main/o/openvpn/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200511-07.xml</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	OpenVPN Client Remote Format String & Denial of Service CVE-2005-3393 CVE-2005-3409	High	<p>Secunia Advisory: SA17376, November 1, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.023, November 2, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p> <p>Debian Security Advisory, DSA 885-1, November 7, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200511-07, November 7, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:206, November 8, 2005</p>
phpMyAdmin phpMyAdmin 2.6.0-2.6.3, 2.5.0-2.5.7, 2.4.0, 2.3.2, 2.3.1, 2.2-2.2.6, 2.1-2.1.2, 2.0-2.0.5	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in 'libraries/auth/cookie.auth.lib.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability has been reported in 'error.php' due to insufficient sanitization of the 'error' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=23067</p> <p>Debian: http://security.debian.org/pool/updates/main/p/phpmyadmin/</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>There is no exploit code</p>	PHPMYAdmin Cross-Site Scripting CVE-2005-2869	Medium	<p>Secunia Advisory: SA16605, August 29, 2005</p> <p>Debian Security Advisory, DSA 880-1, November 2, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p>

	required; however, a Proof of Concept exploit has been published.			
<p>phpMyAdmin</p> <p>phpMyAdmin 2.x</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported due to insufficient verification of certain configuration parameters, which could let a remote malicious user include arbitrary files; and a Cross-Site Scripting vulnerability was reported in 'left.php,' 'queryframe.php,' and 'server_databases.php' due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.4-pl3.tar.gz</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200510-21.xml</p> <p>Debian: http://security.debian.org/pool/updates/main/p/phpmyadmin/</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>phpMyAdmin Local File Inclusion & Cross-Site Scripting</p> <p>CVE-2005-3300 CVE-2005-3301</p>	<p>Medium</p>	<p>Secunia Advisory: SA17289, October 24, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200510-21, October 25, 2005</p> <p>Debian Security Advisory, DSA 880-1, November 2, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p>
<p>Squid Web Proxy</p> <p>Squid Web Proxy Cache 2.5 & prior</p>	<p>A remote Denial of Service vulnerability has been reported in the 'storeBuffer()' function when handling aborted requests.</p> <p>Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE_10-STORE_PENDING.patch</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200509-06.xml</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Debian: http://security.debian.org/pool/updates/main/s/squid/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/s/squid/</p>	<p>Squid Aborted Requests Remote Denial of Service</p> <p>CVE-2005-2794</p>	<p>Low</p>	<p>Security Tracker Alert ID: 1014864, September 7, 2005</p> <p>Gentoo Linux Security Advisory GLSA 200509-06, September 7, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:162, September 12, 2004</p> <p>Debian Security Advisory, DSA 809-1, September 13, 2005</p> <p>Ubuntu Security Notice, USN-183-1, September 13, 2005</p> <p>RedHat Security Advisory, RHSA-2005:766-7, September 15, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:053, September 16, 2005</p> <p>SGI Security Advisory,</p>

	<p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-766.html</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>SGI: ftp://patches.sgi.com/support/free/security/advisories/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>Debian: http://security.debian.org/pool/updates/main/s/squid/</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</p> <p>SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.44</p> <p>Debian: http://security.debian.org/pool/updates/main/s/squid/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			<p>20050903-02-U, September 28, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:1016, September 28, 2005</p> <p>Debian Security Advisory, DSA 809-2, September 30, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-96, October 3, 2005</p> <p>SCO Security Advisory, SCOSA-2005.44, November 1, 2005</p> <p>Debian Security Advisory, DSA 809-3, November 7, 2005</p>
<p>Squid Web Proxy</p> <p>Squid Web Proxy Cache 2.5 .STABLE1-STABLE 10, 2.4 .STABLE6 & 7, STABLE 2, 2.4, 2.3 STABLE 4&5, 2.1 Patch 2, 2.0 Patch 2</p>	<p>A remote Denial of Service vulnerability has been reported in 'squid/src/ssl.c' when a malicious user triggers a segmentation fault in the 'sslConnectTimeout()' function.</p> <p>Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-sslConnectTimeout.patch</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/</p> <p>Debian: http://security.debian.org/pool/updates/</p>	<p>Squid 'sslConnect Timeout()' Remote Denial of Service CVE-2005-2796</p>	Low	<p>Security Tracker Alert ID: 1014846, September 2, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:162, September 12, 2005</p> <p>Ubuntu Security Notice, USN-183-1, September 13, 2005</p> <p>Debian Security Advisory, DSA 809-1, September 13, 2005</p> <p>RedHat Security Advisory, RHSA-2005:766-7, September 15, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:053, September 16, 2005</p> <p>SGI Security Advisory, 20050903-02-U,</p>

	main/s/squid/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-766.html SUSE: ftp://ftp.suse.com/pub/suse/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ SUSE: ftp://ftp.SUSE.com/pub/SUSE SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.44 There is no exploit code required.			September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1016, September 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005 SCO Security Advisory, SCOSA-2005.44, November 1, 2005
Squid Squid 2.x	A remote Denial of Service vulnerability has been reported when handling certain FTP server responses. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE11-rfc1738_do_escape.patch Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.44 SUSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required.	Squid FTP Server Response Handling Remote Denial of Service CVE-2005-3258	Low	Secunia Advisory: SA17271, October 20, 2005 Fedora Update Notifications, FEDORA-2005-1009 & 1010, October 20, 2005 Mandriva Linux Security Advisory, MDKSA-2005:195, October 26, 2005 SCO Security Advisory, SCOSA-2005.44, November 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005
Sylpheed Sylpheed 2.0-2.0.3, 1.0.0-1.0.5	A buffer overflow vulnerability has been reported in 'ldif.c' due to a boundary error in the 'ldif_get_line()' function when importing a LDIF file into the address book, which could let a remote malicious user obtain unauthorized access. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.6.tar.gz	Sylpheed LDIF Import Buffer Overflow CVE-2005-3354	Medium	Bugtraq ID: 15363, November 9, 2005

	Currently we are not aware of any exploits for this vulnerability.			
Todd Miller Sudo 1.x	<p>A vulnerability has been reported in the environment cleaning due to insufficient sanitization, which could let a malicious user obtain elevated privileges.</p> <p>Debian: http://security.debian.org/pool/updates/main/s/sudo/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sudo/</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>There is no exploit code required.</p>	Todd Miller Sudo Local Elevated Privileges CVE-2005-2959	Medium	<p>Debian Security Advisory, DSA 870-1, October 25, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:201, October 27, 2005</p> <p>Ubuntu Security Notice, USN-213-1, October 28, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p>
University of Washington UW-imapd imap-2004c1	<p>A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code.</p> <p>Upgrade to version imap-2004g: ftp://ftp.cac.washington.edu/imap/</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Debian: http://security.debian.org/pool/updates/main/u/uw-imap/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200510-10.xml</p> <p>SUSE: ftp://ftp.SUSE.com/pub/SUSE</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	UW-imapd Denial of Service and Arbitrary Code Execution CVE-2005-2933	High	<p>Secunia, Advisory: SA17062, October 5, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0055, October 7, 2005</p> <p>Debian Security Advisory, DSA 861-1, October 11, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005 US-CERT VU#933601</p> <p>SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:189 & 194, October 21 & 26, 2005</p> <p>Slackware Security Advisory, SSA:2005-310-06, November 7, 2005</p>
up-imapproxy up-imapproxy 1.2.4, 1.2.3	A format string vulnerability has been reported in the 'ParseBannerAnd Capability()' function when processing the banner or capability line received from the IMAP server, which could let a remote malicious user execute	up-imapproxy Format String CVE-2005-2661	High	<p>Debian Security Advisory DSA 852-1, October 9, 2005</p> <p>Security Focus, Bugtraq ID: 15048, November 3, 2005</p>

	arbitrary code. Debian: http://security.debian.org/pool/updates/main/u/up-imapproxy/ A Proof of Concept exploit script has been published.			
Veritas Software VERITAS Cluster Server 2.x, 3.x, 4.x, Storage Foundation 2.x, 3.x, 4.x, Storage Foundation Cluster File System 4.x, Storage Foundation for Database (DB2, Oracle and Sybase) 3.x, 4.x, Storage Foundation for Oracle Real Application Clusters (RAC) 3.x, 4.x	A buffer overflow vulnerability has been reported in the 'ha' command when handling the 'VCSI18N_LANG' environmental variable, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://support.veritas.com/docs/279870 Currently we are not aware of any exploits for this vulnerability.	VERITAS Cluster Server for UNIX Buffer Overflow	High	Symantec Security Advisory, SYM05-023, November 8, 2005
Zope Zope 2.6-2.8.1	A vulnerability has been reported in 'docutils' due to an unspecified error and affects all instances which exposes 'Restructured Text' functionality via the web. The impact was not specified. Hotfix available at: http://www.zope.org/Products/Zope/Hotfix 2005-10-09/security alert/Hot fix_2005-10-09.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-20.xml SUSE: ftp://ftp.suse.com/pub/suse/ Currently we are not aware of any exploits for this vulnerability.	Zope 'Restructured Text' Unspecified Security Vulnerability CVE-2005-3323	Not Specified	Zope Security Alert, October 12, 2005 Gentoo Linux Security Advisory, GLSA 200510-20, October 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005

[\[back to top\]](#)

Multiple Operating Systems - Windows / UNIX / Linux / Other				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Apache	<p>A vulnerability has been reported in Apache which can be exploited by remote malicious users to smuggle http requests.</p> <p>Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000982</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Mandriva: http://www.mandriva.com/security/advisories http://security.ubuntu.com/ubuntu/pool/main/a/apache2/</p>	<p>Apache HTTP Request Smuggling Vulnerability</p> <p>CVE-2005-1268 CVE-2005-2088</p>	Medium	<p>Secunia, Advisory: SA14530, July 26, 2005</p> <p>Conectiva, CLSA-2005:982, July 25, 2005</p> <p>Fedora Update Notification FEDORA-2005-638 & 639, August 2, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005</p> <p>Ubuntu Security Notice, USN-160-1, August 04, 2005</p>

	<p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</p> <p>SGI: ftp://patches.sgi.com/support/free/security/advisories/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>Debian: http://security.debian.org/pool/updates/main/a/apache/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache/</p> <p>SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/</p> <p>IBM has released fixes for Hardware Management Console addressing this issue. Users should contact IBM for further information.</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>			<p>Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005</p> <p>SGI Security Advisory, 20050802-01-U, August 15, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:046, August 16, 2005</p> <p>Debian Security Advisory DSA 803-1, September 8, 2005</p> <p>Ubuntu Security Notice, USN-160-2, September 07, 2005</p> <p>SGI Security Advisory, 20050901-01-U, September 7, 2005</p> <p>Security Focus, Bugtraq ID: 14106, September 21, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0059, October 21, 2005</p> <p>Slackware Security Advisory, SSA:2005-310-04, November 7, 2005</p>
<p>Apache Software Foundation</p> <p>Tomcat 5.5-5.5.12</p>	<p>A remote Denial of Service vulnerability has been reported due to the inefficient generation of directory listing for web directories that have a large number of files.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Apache Tomcat Remote Denial of Service</p> <p>CVE-2005-3510</p>	Low	<p>Security Tracker Alert ID: 1015147, November 3, 2005</p>
<p>Apple</p> <p>QuickTime Player 7.0-7.0.2, 6.5-6.5.2, 6.1, 5.0.2, 6,</p>	<p>Multiple vulnerabilities have been reported: an integer overflow vulnerability was reported when handling a 'Pascal' style string loading a '.mov' video file, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code; an integer overflow vulnerability was reported when handling certain movie attributes when loading a '.mov' video file, which could let a remote malicious user potentially execute arbitrary code; a vulnerability was reported due to a NULL pointer dereferencing error when handling certain missing video file movie attributes, which could let a remote malicious user cause a Denial of Service; and a vulnerability was reported in the QuickTime PictureViewer due to a boundary error when decompressing PICT data, which could let a remote malicious user overwrite memory and potentially execute arbitrary code.</p> <p>Updates available at: http://www.apple.com/support/downloads/quicktime703.html</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>Apple QuickTime Player Integer & Buffer Overflows</p> <p>CVE-2005-2753 CVE-2005-2754 CVE-2005-2755 CVE-2005-2756</p>	High	<p>Security Tracker Alert ID: 1015152, November 4, 2005</p> <p>US-CERT VU#855118</p>
<p>ATutor</p> <p>ATutor 1.5.1 pl2</p>	<p>An SQL injection vulnerability has been reported in 'registration.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit script has been published.</p>	<p>ATutor SQL Injection</p>	Medium	<p>Security Focus, Bugtraq ID: 15355, November 8, 2005</p>
<p>Belchior Foundry</p> <p>vCard Pro 3.1</p>	<p>An SQL injection vulnerability has been reported in 'addrbook.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code.</p>	<p>Belchior Foundry vCard Pro SQL Injection</p>	Medium	<p>Security Focus, Bugtraq ID: 15254, November 1, 2005</p>

	<p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>			
<p>Cisco Systems</p> <p>Cisco 4000 Series Airespace Wireless LAN Controller 3.1.59 .24, 2000 Series Airespace Wireless LAN Controller 3.1.59 .24, Cisco 1240 Series Access Point, 1200 Series Access Point, Cisco 1131 Series Access Point</p>	<p>A vulnerability has been reported in controllers that are in the Lightweight Access Point Protocol (LWAPP) mode of operation because unencrypted traffic is accepted even when configured to encrypt traffic, which could let an unauthorized remote malicious user send unencrypted network packets to a secure network by spoofing the MAC address of another host that has already authenticated.</p> <p>Upgrade information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051102-lwapp.shtml</p> <p>This could be exploited with a publicly available packet crafting or MAC address spoofing utility.</p>	<p>Cisco Airespace Wireless LAN Controller Unencrypted Connections</p> <p>CVE-2005-3482</p>	Medium	<p>Cisco Security Advisory: 68034, November 2, 2005</p>
<p>Cisco Systems</p> <p>Cisco IOS 10.x, 11.x, 12.x, R11.x, R12.x</p>	<p>A buffer overflow vulnerability has been reported when validating whether certain system memory has been corrupted by a heap-based buffer overflow before the internal operating system timers execute code, which could let a remote malicious user execute arbitrary code.</p> <p>Update information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Cisco IOS System Timers Heap Buffer Overflow</p> <p>CVE-2005-3481</p>	High	<p>Cisco Security Advisory: 68064 Rev 1.0-1.2, Updated November 4, 2005</p> <p>US-CERT VU#562945</p>
<p>Cisco Systems</p> <p>CiscoWorks Management Center for IPS Sensors (IPSMC) 2.1</p>	<p>A vulnerability has been reported due to an error in the Cisco IOS IPS (Intrusion Prevention System) configuration file that is generated by the IPS MC and deployed to IOS IPS devices, which could potentially allow malicious traffic to pass through.</p> <p>Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051101-ipsmc.shtml</p> <p>Rev 1.1: Updated information in the Software Versions and Fixes section.</p> <p>There is no exploit code required.</p>	<p>Cisco Management Center for IPS Sensors Signature Disable</p> <p>CVE-2005-3427</p>	Medium	<p>Cisco Security Advisory, 68065, November 1, 2005</p> <p>US-CERT VU#154883</p> <p>Cisco Security Advisory, 68065 Rev1.1, Updated November 3, 2005</p>
<p>CutePHP Team</p> <p>CuteNews 1.4.1</p>	<p>A Directory Traversal vulnerability has been reported in 'show_archives.php' and 'show_news.php' due to insufficient verification of the 'template' parameter before used to include files, which could let a remote malicious user obtain sensitive information and execute arbitrary PHP code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>CutePHP CuteNews Directory Traversal & PHP Code Execution</p> <p>CVE-2005-3507</p>	High	<p>Security Focus, Bugtraq ID: 15295, November 3, 2005</p>
<p>Elite Forum</p> <p>Elite Forum 1.0 .0.0</p>	<p>A vulnerability has been reported due to insufficient sanitization of input when posting a reply, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required;</p>	<p>Elite Forum HTML Injection</p>	Medium	<p>h4cky0u.org Advisory, HYSA-2005-009, November 1, 2005</p>
<p>FRISK Software International</p> <p>F-Prot Antivirus for Windows, Solaris, Linux and BSD 4.4.2, 3.12 d, 3.12 b, Frisk Software Linux, Exchange, BSD, Antivirus 3.16 c</p>	<p>A vulnerability has been reported due to insufficient scanning of decompressed ZIP files that have a header value greater than 15, which could let a remote malicious user bypass the scanning engine.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>F-Prot Antivirus ZIP Attachment Version Scan Bypass</p> <p>CVE-2005-3499</p>	Medium	<p>Security Tracker Alert ID: 1015148, November 3, 2005</p>
<p>F-Secure</p> <p>Internet Gatekeeper 6.4.0-6.42, Anti-Virus for MS Exchange 6.40</p>	<p>A Directory Traversal vulnerability has been reported in the Web Console, which could let a remote malicious user obtain sensitive information.</p> <p>Update information available at: http://www.f-secure.com/security/fsc-2005-2.shtml</p> <p>There is no exploit code required.</p>	<p>F-Secure Web Console Directory Traversal</p>	Medium	<p>F-Secure Security Bulletin FSC-2005-2, November 2, 2005</p>

Gallery Gallery 2.4	<p>An SQL injection vulnerability has been reported in 'ShowGallery.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>Gallery SQL Injection</p> <p>CVE-2005-3508</p>	Medium	Security Focus, Bugtraq ID: 15313, November 4, 2005
IBM Lotus Domino 6.5.0-6.5.4, 6.0-6.0.4, Lotus Domino Web Access (iNotes) 6.x	<p>Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when handling mail rules creation in DWA (Domino Web Access); a remote Denial of Service vulnerability was reported in the Out-Of-Office Agent when processing a message with a From field greater than 256 characters; an unspecified vulnerability was reported in Agents and in MIME to CD conversion; a remote Denial of Service vulnerability was reported when handling invalid HTTP addresses in DWA due to an unspecified error; a remote Denial of Service vulnerability was reported in the mail router when handling a document in the user's mail box that contains an invalid attachment; and a remote Denial of Service vulnerability was reported in Update Task when updating views in the Domino Directory.</p> <p>Updates available at: http://www-10.lotus.com/ldd/r5fixlist.nsf/8c4f0b18f61ab80585256cb400719709/59999026d2bf23e8852570a5006b0a5d?OpenDocument</p> <p>Some of these vulnerabilities do not require exploit code.</p>	IBM Lotus Domino/Notes Multiple Vulnerabilities	Low	Secunia Advisory: SA17429, November 4, 2005
IBM Tivoli Access Manager for Business Integration 5.x, Tivoli Access Manager for e-business 5.x, Tivoli Access Manager for Operating Systems 5.x, Tivoli Directory Integrator 5.x, 6.x, Tivoli Directory Server 5.x, 6.x, Tivoli Federated Identity Manager 6.x, Tivoli Identity Manager 4.x	<p>A vulnerability has been reported in the server's 'slapd' daemon due to an unspecified error, which could let a remote malicious user obtain unauthorized access and change, modify and/or delete directory data.</p> <p>Update information available at: http://www-1.ibm.com/support/docview.wss?uid=swg21221665</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	IBM Tivoli Directory Server Security Bypass	Medium	IBM Security Advisory, November 9, 2005
IBM Websphere Application Server 5.1.1 .4, 5.1.1 .3	<p>A vulnerability has been reported in the log file when tracing for the session manager is enabled because the 'QueryString' is logged when a URL is encoded, which could let a remote malicious user obtain sensitive information.</p> <p>Update information available at: http://www-1.ibm.com/support/docview.wss?uid=swg24010781</p> <p>There is no exploit code required.</p>	<p>IBM WebSphere Application Server Information Disclosure</p> <p>CVE-2005-3498</p>	Medium	Security Tracker Alert ID: 1015134, November 2, 2005
ibProArcade ibProArcade 2.5.2	<p>An SQL injection vulnerability has been reported in the 'report' module due to insufficient sanitization of input in the 'user' parameter in 'index.php' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>Update available at: http://www.ibproarcade.com/</p> <p>A Proof of Concept exploit has been published.</p>	ibProArcade Module SQL Injection	Medium	Secunia Advisory: SA17457, November 7, 2005
Invision Power Services Invision Board 2.1	<p>Several vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported due to insufficient of unspecified input in the administration interface before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and multiple HTML injection vulnerabilities were reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	Invision Power Board Multiple Cross-Site Scripting & HTML Injection	Medium	Security Focus, Bugtraq ID: 15344 & 15345, November 7, 2005

Jelsoft Enterprises VBulletin 3.0-3.0.9, 2.3.0-2.3.4, 2.2.0-2.2.9, 2.0.3, 2.0 rc 2& rc 3, 1.0.1 lite	<p>An input validation vulnerability has been reported in the image upload handling, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Update available at: http://www.vbulletin.com/forum/showthread.php?t=161721</p> <p>There is no exploit code required.</p>	vBulletin Image Upload Input Validation	Medium	Security Focus, Bugtraq ID: 15296, November 3, 2005
Johannes F. Kuhlmann FlatFrag 0.3 & prior	<p>Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to insufficient bounds checking of user-supplied data before coping to an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code: and a remote Denial of Service vulnerability was reported due to an attempt to dereference a NULL pointer.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	<p>Johannes F. Kuhlmann FlatFrag Remote Buffer Overflow & Denial of Service</p> <p>CVE-2005-3491 CVE-2005-3492</p>	High	Security Focus, Bugtraq ID: 15287, November 2, 2005
JPortal JPortal Web Portal 2.3.1, 2.2.1	<p>Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>JPortal Multiple SQL Injection</p> <p>CVE-2005-3509</p>	Medium	Security Focus, Bugtraq ID: 15324, November 4, 2005
Macromedia Flash 7.0.19 .0, 7.0 r19, 6.0.79 .0, 6.0.65 .0, 6.0.47 .0, 6.0.40 .0, 6.0.29 .0, 6.0	<p>A vulnerability has been reported due to insufficient validation of the frame type identifier that is read from a SWF file, which could let a remote malicious user execute arbitrary code.</p> <p>Update information available at: http://www.macromedia.com/devnet/security/security_zone/mpsb05-07.html</p> <p>An exploit has been published.</p>	<p>Macromedia Flash Array Index Remote Arbitrary Code Execution</p> <p>CVE-2005-2628</p>	High	Macromedia Security Advisory, MPSB05-07, November 5, 2005
Macromedia Flash 7.0.19 .0 & prior	<p>An input validation vulnerability has been reported in 'ActionDefineFunction' due to an error for a critical array index value, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.</p> <p>Update information available at: http://www.macromedia.com/devnet/security/security_zone/mpsb05-07.html</p> <p>A Proof of Concept exploit has been published.</p>	Macromedia Flash Input Validation	High	Macromedia Security Bulletin, MPSB05-07, November 7, 2005

<p>Mozilla.org</p> <p>Netscape 8.0.3.3, 7.2; Mozilla Firefox 1.5 Beta1, 1.0.6; Mozilla Browser 1.7.11; Mozilla Thunderbird 1.0.6</p>	<p>A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code.</p> <p>Patches available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-769.html</p> <p>http://rhn.redhat.com/errata/RHSA-2005-768.html</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</p> <p>HP: http://software.hp.com/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>HPSBUX01231 Rev1: Preliminary Mozilla 1.7.12 available.</p> <p>Netscape: http://browser.netscape.com/ns8/download/default.jsp</p> <p>Debian: http://security.debian.org/pool/updates/main/m/mozilla/</p> <p>http://security.debian.org/pool/updates/main/m/mozilla-</p>	<p>Mozilla/Netscape/ Firefox Browsers Domain Name Buffer Overflow</p> <p>CVE-2005-2871</p>	<p>High</p> <p>Security Focus, Bugtraq ID: 14784, September 10, 2005</p> <p>RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005</p> <p>Ubuntu Security Notice, USN-181-1, September 12, 2005</p> <p>US-CERT VU#573857</p> <p>Gentoo Linux Security Advisory GLSA 200509-11, September 18, 2005</p> <p>Security Focus, Bugtraq ID: 14784, September 22, 2005</p> <p>Slackware Security Advisory, SSA:2005-269-01, September 26, 2005</p> <p>Gentoo Linux Security Advisory [UPDATE], GLSA 200509-11:02, September 29, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005</p> <p>Debian Security Advisory, DSA 837-1, October 2, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005</p> <p>HP Security Bulletin, HPSBUX01231, October 3, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005</p> <p>HP Security Bulletin, HPSBUX01231 Rev 1, October 12, 2005</p> <p>Debian Security Advisories, DSA 866-1 & 868-1, October 20, 2005</p> <p>HP Security Bulletin, HPSBUX01231 Rev 2, November 9, 2005</p>
--	---	--	---

	<p>thunderbird/</p> <p>HPSBUX01231 Rev.2: HP-UX Mozilla Remote Unauthorized Execution of Privileged Code or Denial of Service (DoS)) is available detailing information on the availability of version 1.7.12.01 of Mozilla for various HP platforms. Users should see the referenced advisory or contact HP for further information.</p> <p>A Proof of Concept exploit script has been published.</p>			
<p>Multiple Vendors</p> <p>MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2; Gentoo Linux; Ethereal Group Ethereal 0.10.1-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7</p>	<p>A vulnerability has been reported in Ethereal, IRC Protocol Dissector, that could let remote malicious users cause a Denial of Service.</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200510-25.xml</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Ethereal Denial of Service</p> <p>CVE-2005-3313</p>	<p>Low</p>	<p>Mandriva Linux Security Advisory, MDKSA-2005:193-1, October 26, 2005</p> <p>Gentoo Linux Security Advisor, GLSA 200510-25, October 30, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p> <p>Conectiva Security Announce-ment, CLSA-2005:1043, November 8, 2005</p>
<p>Multiple Vendors</p> <p>Mozilla Firefox 1.5 beta 1 & beta 2, 1.0-1.0.7, 0.10.1, 0.10, 0.9-0.9.3, 0.8, Firefox Preview Release; Browser 1.8 Alpha 1-Alpha 4, 1.7-1.7.12, 1.6, 1.5.1, 1.5, 1.4.4, 1.4.2, 1.4.1, 1.4 1 & b, 1.4, 1.3.1, 1.3, 1.2.1, 1.2, Alpha & Beta, 1.1, Alpha & Beta, 1.0-1.0.2, 0.9.48, 0.9.35, 0.9.2-0.9.9, 0.8, M16, M15; KDE Konqueror Embedded 0.1, Konqueror 3.3-3.3.2, 3.2.3, 3.2.2 -6, 3.2.1, 3.1-3.1.5, 3.0.5 b, 3.0.5, 3.0- 3.0.3, 2.2.2, 2.2.1, 2.1.2, 2.1.1</p>	<p>A vulnerability has been reported due to a failure to ensure that cookies are properly associated to domain names, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Multiple Vendor Web Browser Cookie Hostname Information Disclosure</p>	<p>Medium</p>	<p>Security Focus, Bugtraq ID: 15331, November 4, 2005</p>
<p>Multiple Vendors</p> <p>PHPXMLRPC 1.1.1; PEAR XML_RPC 1.3.3; Drupal 4.6-4.6.2, 4.5- 4.5.4; Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.; MailWatch for MailScanner 1.0.1; eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0</p>	<p>A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code.</p> <p>PHPXMLRPC : http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc.1.2.tgz?download</p> <p>Pear: http://pear.php.net/get/XML_RPC-1.4.0.tgz</p> <p>Drupal: http://drupal.org/files/projects/drupal-4.5.5.tar.gz</p> <p>eGroupWare: http://prdownloads.sourceforge.net/egroupware/eGroupWare-1.0.0.009.tar .gz?download</p> <p>MailWatch: http://prdownloads.sourceforge.net/mailwatch/</p>	<p>PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution</p> <p>CVE-2005-2498</p>	<p>High</p>	<p>Security Focus, Bugtraq ID 14560, August 15, 2005</p> <p>Security Focus, Bugtraq ID 14560, August 18, 2005</p> <p>RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005</p> <p>Ubuntu Security Notice, USN-171-1, August 20, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:146, August 22, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200508-13 & 14, & 200508-18, August 24 & 26, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-809 & 810, August 25, 2005</p>

[mailwatch-1.0.2.tar.gz](#)

Nucleus:

<http://prdownloads.sourceforge.net/nucleuscms/nucleus-xmlrpc-patch.zip?download>

RedHat:

<http://rhn.redhat.com/errata/RHSA-2005-748.html>

Ubuntu:

<http://security.ubuntu.com/ubuntu/pool/main/p/php4/>

Mandriva:

<http://www.mandriva.com/security/advisories>

Gentoo:

<http://security.gentoo.org/glsa/glsa-200508-13.xml>

<http://security.gentoo.org/glsa/glsa-200508-14.xml>

<http://security.gentoo.org/glsa/glsa-200508-18.xml>

Fedora:

<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/>

Debian:

<http://security.debian.org/pool/updates/main/p/php4/>

SUSE:

<ftp://ftp.suse.com/pub/suse/>

Gentoo:

<http://security.gentoo.org/glsa/glsa-200508-20.xml>

<http://security.gentoo.org/glsa/glsa-200508-21.xml>

Slackware:

<ftp://ftp.slackware.com/pub/slackware/>

Debian:

<http://security.debian.org/pool/updates/main/p/phpgroupware/>

SGI:

ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/

Slackware:

<ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/>

<ftp://ftp.slackware.com/pub/slackware/slackware-10.1/testing/packages/php-5.0.5/php-5.0.5>

Debian Security Advisory, DSA 789-1, August 29, 2005

SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005

Gentoo Linux Security Advisory, GLSA GLSA 200508-20& 200508-21, August 30 & 31, 2005

Slackware Security Advisory, SSA:2005-242-02, August 31, 2005

Debian Security Advisory, DSA 798-1, September 2, 2005

SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005

SGI Security Advisory, 20050901-01-U, September 7, 2005

Slackware Security Advisories, SSA:2005-251-03 & 251-04, September 9, 2005

Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005

Debian Security Advisory, DSA 840-1, October 4, 2005

Debian Security Advisory, DSA 842-1, October 4, 2005

Conectiva Linux Announcement, CLSA-2005:1024, October 7, 2005

Security Focus, Bugtraq ID: 14560, November 7, 2005

	<p>-i486-1.tgz</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200509-19.xml</p> <p>Debian: http://security.debian.org/pool/updates/main/d/drupal/</p> <p>Debian: http://security.debian.org/pool/updates/main/e/egroupware/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>b2evolution: http://prdownloads.sourceforge.net/evocms/b2evolution-0.9.1b-2005-09-16.zip?download</p> <p>There is no exploit code required.</p>			
<p>Multiple Vendors</p> <p>PunBB 1.2.1-1.2.9; BLOG:CMS 4.0 .0-4.0 .0d, 3.6.4, 3.6.2, 3.1-3.1.4, 3.0</p>	<p>Several vulnerabilities have been reported: a HTML injection vulnerability was reported when uploading images due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported because addresses can be hidden that use the 'X_FORWARDED_FOR' field in the HTTP header, which could let a remote malicious user spoof the origin; and an unspecified information disclosure vulnerability was reported.</p> <p>PunBB: http://www.punbb.org/download/punbb-1.2.10.tar.gz</p> <p>Blog:CMS: http://prdownloads.sourceforge.net/blogcms/blogcms.4.0.0e.tgz</p> <p>There is no exploit code required.</p>	PunBB/Blog:CMS HTML Injection, Origin Spoof & Information Disclosure	Medium	Security Focus, Bugtraq IDs: 15322, 15326, & 15328, November 4, 2005
<p>Multiple Vendors</p> <p>RedHat Fedora Core4, Core3; PHP 5.0.4, 4.3.9</p>	<p>A remote Denial of Service vulnerability has been reported when parsing EXIF image data contained in corrupt JPEG files.</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	PHP Group Exif Module Remote Denial of Service CVE-2005-3353	Low	Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005
<p>Multiple Vendors</p> <p>RedHat Fedora Core4, Core3; Ethereal Group Ethereal 0.10 -0.10.12, 0.9-0.9.16, 0.8.19, 0.8.18</p>	<p>Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the ISAKMP, FC-FCS, RSVP, and ISIS LSP dissectors; a remote Denial of Service vulnerability was reported in the IrDA dissector; a buffer overflow vulnerability was reported in the SLIMP3, AgentX, and SRVLOC dissectors, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in the BER dissector; a remote Denial of Service vulnerability was reported in the SigComp UDVM dissector; a remote Denial of service vulnerability was reported due to a null pointer dereference in the SCSI, sFlow, and RTnet dissectors; a vulnerability was reported because a remote malicious user can trigger a divide by zero error in the X11 dissector; a vulnerability was reported because a remote malicious user can cause an invalid pointer to be freed in the WSP dissector; a remote Denial of Service vulnerability was reported if the 'Dissect unknown RPC program numbers' option is enabled (not the default setting); and a remote Denial of Service vulnerability was reported if SMB transaction payload reassembly is enabled (not the default setting).</p> <p>Upgrades available at: http://prdownloads.sourceforge.net/ethereal/ethereal-0.10.13.tar.gz?download</p>	Ethereal Multiple Protocol Dissector Vulnerabilities CVE-2005-3184 CVE-2005-3241 CVE-2005-3242 CVE-2005-3243 CVE-2005-3244 CVE-2005-3245 CVE-2005-3246 CVE-2005-3247 CVE-2005-3248 CVE-2005-3249	High	<p>Ethereal Security Advisory, enpa-sa-00021, October 19, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-1008 & 1011, October 20, 2005</p> <p>RedHat Security Advisory, RHSA-2005:809-6, October 25, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:193, October 25, 2005</p> <p>Avaya Security Advisory, ASA-2005-227, October 28, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200510-25, October 30, 2005</p>

Fedora:
[http://download.fedora.
redhat.com/pub/fedora/
linux/core/updates/](http://download.fedora.redhat.com/pub/fedora/linux/core/updates/)

RedHat:
[http://rhn.redhat.com/
errata/RHSA-
2005-809.html](http://rhn.redhat.com/errata/RHSA-2005-809.html)

Mandriva:
[http://www.mandriva.com/
security/advisories](http://www.mandriva.com/security/advisories)

Avaya:
[http://support.avaya.
com/elmodocs2/
security/ASA-
2005-227.pdf](http://support.avaya.com/elmodocs2/security/ASA-2005-227.pdf)

Gentoo:
[http://security.gentoo.
org/glsa/glsa-
200510-25.xml](http://security.gentoo.org/glsa/glsa-200510-25.xml)

SUSE:
[ftp://ftp.suse.com
/pub/suse/](ftp://ftp.suse.com/pub/suse/)

An exploit script has been published.

Mandriva Linux Security
Advisory,
MDKSA-2005:193-2,
October 31, 2005

**SUSE Security Summary
Report,
SUSE-SR:2005:025,
November 4, 2005**

<p>Multiple Vendors</p> <p>University of Kansas Lynx 2.8.6 dev.1-dev.13, 2.8.5 dev.8, 2.8.5 dev.2-dev.5, 2.8.5, 2.8.4 rel.1, 2.8.4, 2.8.3 rel.1, 2.8.3 pre.5, 2.8.3 dev2x, 2.8.3 dev.22, 2.8.3, 2.8.2 rel.1, 2.8.1, 2.8, 2.7;</p> <p>RedHat Enterprise Linux WS 4, WS 3, 2.1, ES 4, ES 3, ES 2.1, AS 4, AS 3, AS 2.1,</p> <p>RedHat Desktop 4.0, 3.0,</p> <p>RedHat Advanced Workstation for the Itanium Processor 2.1 IA64</p>	<p>A buffer overflow vulnerability has been reported in the 'HTrjis()' function when handling NNTP article headers, which could let a remote malicious user execute arbitrary code.</p> <p>University of Kansas Lynx: http://lynx.isc.org/current/lynx2.8.6dev.14.tar.gz</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200510-15.xml</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lynx/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-803.html</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/10/</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>SGI: http://www.sgi.com/support/security/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Debian: http://security.debian.org/pool/updates/main/l/lynx/</p> <p>http://security.debian.org/pool/updates/main/l/lynx-ssl/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lynx/</p> <p>(Note: Ubuntu advisory USN-206-1 was previously released to address this vulnerability, however, the fixes contained an error that caused lynx to crash.)</p> <p>SUSE: ftp://ftp.suse.com/pub/suse/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.47</p> <p>A Proof of Concept Denial of Service exploit script has been published.</p>	<p>Lynx 'HTrjis()' NNTP Remote Buffer Overflow</p> <p>CVE-2005-3120</p>	<p>High</p> <p>Gentoo Linux Security Advisory, GLSA 200510-15, October 17, 2005</p> <p>Ubuntu Security Notice, USN-206-1, October 17, 2005</p> <p>RedHat Security Advisory, RHSA-2005:803-4, October 17, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-993 & 994, October 17, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:186, October 18, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:1037, October 19, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005</p> <p>SGI Security Advisory, 20051003-01-U, October 26, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:186-1, October 26, 2005</p> <p>Debian Security Advisories, DSA 874-1 & 876-1, October 27, 2005</p> <p>Ubuntu Security Notice, USN-206-2, October 29, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p> <p>Slackware Security Advisory, SSA:2005-310-03, November 7, 2005</p> <p>SCO Security Advisory, SCOSA-2005.47, November 8, 2005</p>
<p>Multiple Vendors</p> <p>Xoops 2.0.10-2.0.12, 2.0.9.3, 2.0.9.2, 2.0.5-2.0.5.2, 2.0- 2.0.3;</p> <p>XML-RPC for PHP</p> <p>XML-RPC for PHP 1.1,</p>	<p>A vulnerability was reported due to insufficient sanitization of the 'eval()' call, which could let a remote malicious user execute arbitrary PHP code.</p> <p>Drupal: http://drupal.org/files/projects/drupal-</p>	<p>Multiple Vendors XML-RPC for PHP Remote Code Injection</p> <p>CVE-2005-1921</p>	<p>High</p> <p>Security Focus, 14088, June 29, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-01, July 3, 2005</p>

1.0.99 .2, 1.0.99, 1.0-1.02; WordPress 1.5-1.5.1 .2, 1.2-1.2.2, 0.71,0.7; S9Y Serendipity 0.8.1, 0.8 -beta6 Snapshot, 0.8 -beta5 & beta6, 0.8; PostNuke Development Team PostNuke 0.76 RC4a&b, RC4, 0.75; phpMyFAQ 1.5 RC1-RC4, 1.5 beta1-beta3, 1.5 alpha1&2, 1.4-1.4.8, 1.4; PEAR XML_RPC 1.3 RC1-RC3, 1.3; MandrakeSoft Linux Mandrake 10.2 x86_64, 10.2, 10.1 x86_64, 10.1, 10.0 amd64, 10.0, Corporate Server 3.0 x86_64, 3.0; Drupal 4.6.1, 4.6, 4.5- 4.5.3	<p>4.5.4.tar.gz</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>Pear: http://pear.php.net/get/XML_RPC-1.3.1.tgz</p> <p>PhpMyFaq: http://freshmeat.net/redirect.phpmyfaq/38789/url_zip/download.php</p> <p>S9Y Serendipity: http://prdownloads.sourceforge.net/php-blog/serendipity-0.8.2.tar.gz?download</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>WordPress: http://wordpress.org/latest.zip</p> <p>XML-RPC: http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc-1.1.1.tgz?download</p> <p>Xoops: http://www.xoops.org/modules/core/visit.php?cid=3&lid=62</p> <p>Gentoo: http://security.gentoo.org/glsa/glsa-200507-01.xml http://security.gentoo.org/glsa/glsa-200507-06.xml http://security.gentoo.org/glsa/glsa-200507-07.xml http://security.gentoo.org/glsa/glsa-200507-15.xml</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/</p> <p>Debian: http://security.debian.org/pool/updates/main/d/drupal/ http://security.debian.org/pool/updates/main/p/phpgroupware/ http://security.debian.org/pool/updates/main/e/egroupware/</p> <p>SGI: http://www.sgi.com/support/security/</p> <p>SuSE: ftp://ftp.SUSE.com/pub/SUSE</p> <p>Trustix: http://http.trustix.org/pub/trustix/updates/</p> <p>Debian:</p>	<p>Fedora Update Notifications, FEDORA-2005-517 & 518, July 5, 2006</p> <p>Ubuntu Security Notice, USN-147-1 & USN-147-2, July 05 & 06, 2005</p> <p>US-CERT VU#442845</p> <p>Gentoo Linux Security Advisory, GLSA 200507-06, July 6, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-07, July 10, 2005</p> <p>SuSE Security Announcement, SUSE-SA:2005:041, July 8, 2005</p> <p>Debian Security Advisories, DSA 745-1, 747-1, & DSA 746-1, July 10 & 13, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005</p> <p>SGI Security Advisory, 20050703-01-U, July 15, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-15, July 15, 2005</p> <p>Debian Security Advisory, DSA 789-1, August 29, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005</p> <p>Security Focus, Bugtraq ID: 14088, November 7, 2005</p>
---	---	--

	http://security.debian.org/pool/updates/main/p/php4/ SUSE: ftp://ftp.suse.com/pub/suse/ MAXdev MD-Pro Content Management: http://www.maxdev.com/Downloads-index-reg-viewdownload-cid-3.phtml b2evolution: http://prdownloads.sourceforge.net/evocms/b2evolution-0.9.1b-2005-09-16.zip?download Exploit scripts have been published.			
OSTE OSTE 1.x	A vulnerability has been reported in 'index.php' due to insufficient verification of the 'page' and 'site' parameters before including files, which could let a remote malicious user execute arbitrary remote PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	OSTE File Inclusion Vulnerability	High	Secunia Advisory: SA17493, November 8, 2005
PHP Handicapper PHP Handicapper	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'process_signup.php' due to insufficient sanitization of the 'login' parameter and in 'msg.php' due to insufficient sanitization of the 'msg' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'process_signup.php' due to insufficient sanitization of the 'serviceid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP Handicapper Cross-Site Scripting & SQL Injection CVE-2005-3496 CVE-2005-3497	Medium	Secunia Advisory: SA17412, November 3, 2005
PHP PHP 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 5.0.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of the 'GLOBALS' array, which could let a remote malicious user define global variables; a vulnerability was reported in the 'parse_str()' PHP function when handling an unexpected termination, which could let a remote malicious user enable the 'register_globals' directive; a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an integer overflow vulnerability was reported in 'pcrelib' due to an error, which could let a remote malicious user corrupt memory. Upgrades available at: http://www.php.net/get/php-4.4.1.tar.gz SUSE: ftp://ftp.suse.com/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ There is no exploit code required.	PHP Multiple Vulnerabilities CVE-2005-3388 CVE-2005-3389 CVE-2005-3390 CVE-2005-3391 CVE-2005-3392	Medium	Secunia Advisory: SA17371, October 31, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005
phpBB Group phpBB 2.0-2.0.18, 1.4.4, 1.4.0-1.4.2, 1.2.1, 1.2.0, 1.0.0	A Cross-Site Scripting vulnerability has been reported in 'Usercp_sendpasswd.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPBB Forum Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 15357, November 8, 2005
PHPFM PHPFM	A file upload vulnerability has been reported, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing.	PHPFM Arbitrary File Upload	Medium	Security Focus, Bugtraq ID: 15335, November 7, 2005

	There is no exploit code required; however, a Proof of Concept exploit has been published.			
PHPKIT PHPKIT 1.6.1 R2 & prior	<p>Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in 'admin/admin.php' due to insufficient sanitization of the 'site_body' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported due to insufficient sanitization of the referer HTTP header, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported in the 'id' and 'PHPKITSID' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in the 'path' parameter in various scripts due to insufficient verification before used to include files, which could let a remote malicious user execute arbitrary PHP code; and a vulnerability was reported in the 'eval()' call due to insufficient sanitization, which could let a remote malicious user execute arbitrary PHP code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	PHPKit Multiple Input Validation	High	Hardened PHP Project Security Advisory, November 7, 2005
PHPList PHPList Mailing List Manager 2.10.1, 2.8.12, 2.6-2.6.4	<p>Multiple vulnerabilities have been reported: a vulnerability was reported because users can access other users' personal details; a vulnerability was reported in the sign up process, which could let a remote malicious user obtain access without providing a password; a vulnerability was reported due to insufficient sanitization of some input in the administration interface before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported due to insufficient sanitization of some input in the administration interface before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported due to insufficient sanitization of some input passed in the administration interface before displaying, which could let a remote malicious user obtain sensitive information.</p> <p>Upgrades available at: http://prdownloads.sourceforge.net/phplist/phplist-2.10.2.tgz?download</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	PHPList Multiple Input Validation	Medium	Secunia Advisory: SA17476, November 8, 2005
PhpWeb Things PhpWebThings 0.4.4	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'forum.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'Forum.PHP' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	phpWebThings Cross-Site Scripting & SQL Injection	Medium	Security Focus, Bugtraq ID: 15276 & 15277, November 2, 2005
SAP SAP Web Application Server 7.0, 6.40, 6.20, 6.10	<p>Several vulnerabilities have been reported: an HTTP response splitting vulnerability was reported due to insufficient sanitization of user-supplied input, which could lead to a false sense of trust; several Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a URI redirection vulnerability was reported in the 'sap-exiturl' parameter, which could let a remote malicious user steal cookie-based credentials or enhance phishing style attacks.</p> <p>The vendor has released solutions and patch information regarding this issue. Users are advised to contact the vendor for further information.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published for the Cross-Site Scripting & URI Redirection vulnerabilities.</p>	SAP Web Application Server HTTP Response Splitting, Cross-Site Scripting & URI Redirection	Medium	Security Focus, Bugtraq ID: 15360, 15361, & 15362, November 9, 2005

Scorched 3D Scorched 3D 39.1, 37.1, 37.0, 36.0-36.2, 35.0	<p>Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to boundary and format string errors in various functions, which could let a remote malicious user execute arbitrary code; a vulnerability as reported in 'ServerConnect Handler.cpp' due to an error when handing the 'numplayers' field, which could let a remote malicious user freeze a vulnerable server; a buffer overflow vulnerability was reported in 'ComsMessage Handler.cpp' due to an error when creating error messages, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported in 'Logger.cpp' due to an error when handling overly large values.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	Scorched 3D Multiple Vulnerabilities CVE-2005-3486 CVE-2005-3487 CVE-2005-3488	High	Secunia Advisory: SA17423, November 4, 2005
Six Apart Movable Type 3.17, 3.16, 3.2, 2.63, 2.0	<p>Several vulnerabilities have been reported; a vulnerability was reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user create an arbitrary blog path; and a vulnerability was reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>There is no exploit code required.</p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	Movable Type Arbitrary Blog Creation Path & Entry Posting HTML Injection	Medium	Security Focus, Bugtraq ID: 15302 & 15305, November 3, 2005
SquirrelMail SquirrelMail 1.4.0-1.4.5-RC1.	<p>A vulnerability has been reported in 'options_identities.php' because parameters are insecurely extracted, which could let a remote malicious user execute arbitrary HTML and script code, or obtain/ manipulate sensitive information.</p> <p>Upgrades available at: http://www.squirrelmail.org/download.php</p> <p>Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/</p> <p>RedHat: http://rhn.redhat.com/errata/RHSA-2005-595.html</p> <p>Apple: http://docs.info.apple.com/article.html?artnum=302163</p> <p>Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</p> <p>Fedora: http://download.fedoralegacy.org/fedora/</p> <p>Mandriva: http://www.mandriva.com/security/advisories</p> <p>There is no exploit code required.</p>	SquirrelMail Variable Handling CVE-2005-2095	Medium	<p>GulfTech Security Research Advisory, July 13, 2005</p> <p>Debian Security Advisory, DSA 756-1, July 13, 2005</p> <p>RedHat Security Advisory, RHSA-2005:595-12, August 3, 2005</p> <p>Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-779 & 780, August 22, 2005</p> <p>Fedora Legacy Update Advisory, FLSA:163047, September 15, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:202, November 2, 2005</p>
Sun Microsystems, Inc. JDK (Windows Production Release) 1.5.0_05, 1.4.2_09, 1.4.2_08, JDK (Solaris Production Release) 1.5.0_05, 1.4.2_09, 1.4.2_08, JDK (Linux Production Release) 1.5.0_05, 1.4.2_09, 1.4.2_08, JDK 1.5 .0_05, 1.4.2_09, 1.4.2_08	<p>A remote Denial of Service vulnerability has been reported due to a font deserialization error.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability</p>	Sun Java Development Kit Font Serialization Remote Denial of Service	Low	Security Focus, Bugtraq ID: 15312, November 4, 2005

The XMB Group XMB Forum 1.9.3	<p>A Cross-Site Scripting vulnerability has been reported in 'u2u.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	XMB Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 15342, November 7, 2005
The XMB Group XMB Forum 1.9.3	<p>An SQL injection vulnerability has been reported in 'post.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	XMB Forum SQL Injection	Medium	Security Focus, Bugtraq ID: 15267, November 1, 2005
toendaCMS toendaCMS 0.6.1	<p>Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in 'admin.php' due to insufficient verification of the 'id_user' parameter before used to display files, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported because user credentials and session information is stored inside the web root, which could let a remote malicious user obtain sensitive information.</p> <p>Upgrade available at: http://www.toenda.com/de/data/files/Software/toendaCMS_Version_0.6.0_Stable/toendaCMS_0.6.2_Stable.zip</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	toendaCMS Information Disclosure	Medium	SEC-CONSULT Security Advisory, November 7, 2005
Veritas Software NetBackup Server 5.1, 5.0, NetBackup Enterprise Server 5.1, 5.0, NetBackup Client 5.1, 5.0	<p>A buffer overflow vulnerability has been reported in a shared library used by the VERITAS NetBackup volume manager daemon (vmd), which could let a remote malicious user potentially execute arbitrary code or cause a Denial of Service.</p> <p>Patches available at: http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNLOAD.htm</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>VERITAS NetBackup Volume Manager Daemon Buffer Overflow</p> <p>CVE-2005-3116</p>	High	Symantec Security Advisory, SYM05-024, November 8, 2005
Vubb Vubb	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a path disclosure vulnerability has been reported when an error message is displayed, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit script has been published.</p>	<p>VUBB Cross-Site Scripting & Path Disclosure</p> <p>CVE-2005-3512 CVE-2005-3513</p>	Medium	KAPDA Advisory :#10, November 1, 2005
WebGroup Media Cerberus Helpdesk 2.6.1, 2.0-2.5	<p>A vulnerability has been reported in the 'attachment_send.php' script due to insufficient authentication when accessing tickets, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Cerberus Helpdesk Information Disclosure</p> <p>CVE-2005-3502</p>	Medium	Security Tracker Alert ID: 1015153, November 4, 2005
YaBB YaBB 2.0, RC1 & RC2, 1.41, 1.40, YaBB 1 Gold Release, SP 1.4, SP 1.3-1.3.2, SP 1.2, SP 1	<p>A vulnerability has been reported in the attachment upload handling due to an input validation error, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Upgrades available at: http://www.yabbforum.com/downloads.php?file=YaBB_2.1.zip</p> <p>There is no exploit code required.</p>	YaBB Image Upload HTML Injection	Medium	Secunia Advisory: SA17411, November 9, 2005

- **IDC: As mobile workforce grows, IT support could lag:** According to a study by IDC, the global mobile workforce is expected to grow by more than 20% in the next four years, with 878 million mobile workers toiling away on laptops, handhelds and cell phones by 2009. However, IT managers today often don't deal with the complexities associated with managing, securing and supporting handheld devices and applications for mobile workers. Source: <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,106062,00.html>.
- **Agencies jockey over wireless spectrum:** By the end of this month, federal agencies will release to the Commerce Department plans on how they will manage their allotment of the nation's airwaves. Since President Bush unveiled a sweeping spectrum management memorandum last December that included 24 recommendations and key milestones, federal agencies have been scrambling to determine how much of the electromagnetic spectrum they are using and for what purposes. Source: http://www.gcn.com/vol1_no1/daily-updates/37475-1.html.
- **New type of phishing could hit mobile phone users:** Experts are warning that a new type of phishing that could siphon bank details from mobile phone users. Mophophishing is where hackers send out fake banking applications to unsuspecting mobile phone users. The users then type their account details into the application thinking they were accessing their accounts when they were actually sending their personal details back to the hacker. Spotting a phishing email is relatively straightforward, the user need only examine the source code of an HTML email and inspect the domain name and path of any link to verify its authenticity. But with a mobile application, this information is concealed deep within the application code itself. Source: <http://www.scmagazine.com/uk/news/article/525582/new-type-phishing-hit-mobile-phone-users/>

Wireless Vulnerabilities

- **Cisco flaw puts Wi-Fi networks at risk:** This problem affects large Wi-Fi networks and occurs when Cisco 1200, 1131 and 1240 series Wi-Fi access points are controlled by Cisco 2000 and 4400 series Airespace Wireless LAN Controllers. Source: http://news.com.com/Cisco+flaw+puts+Wi-Fi+networks+at+risk/2100-7349_3-5929059.html?tag=cd.top
- **ssf.zip:** A VoIP Phone exploit tool.
- **WifiScanner-1.0.1.tar.gz:** An analyzer and detector of 802.11b stations and access points.
- **phzine01.zip:** Phearless Serbian/Croatian Security Magazine Issue #01.

[\[back to top\]](#)

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 9, 2005	advisory_212005.80.txt	No	Sample exploitation for the PHPKit Multiple Input Validation vulnerabilities.
November 9, 2005	phzine01.zip	N/A	Phearless Serbian/Croatian Security Magazine Issue #01 Included in this issue: The Art of Sniffing, The Art of Footprinting, SQL Injection Techniques, Wireless - Under the hood, Cross Site Scripting with examples, VX Coding - New ideas, Win Hack and Tweak, Samba Lin and Win Dance, Exploiting ShopAdmin, CGI Exploiting, and Mirc Scripting Basics.
November 9, 2005	phzine02.zip	N/A	Phearless Serbian/Croatian Security Magazine Issue #02. Included in this issue: Symbian OS - Under the Hood, Runtime Decryption and Meta Swap Engine, BlackHand.w32(DeadCode.a/b) Analysis, prc-ko - the 4th Native API virus, NT Startup Methods Exposed, Phearless Challenge #2: Reversme, Full Reverse(Target VCT #1), Full Reverse(Target VCT #2), Full Reverse(Target VCT #3), Writing Linux Shellcode - Basics, Hiding Behind Firewall, Phreaking in Serbia, Cryptology 101, Win Hacks and Tips #2, and Security from iso/osi Reference Model Perspective.
November 9, 2005	phzine03.zip	N/A	Phearless Serbian/Croatian Security Magazine Issue #03. Included in this issue: Injecting Malware: Symbian Micro Kernel, Smart EPO Techniques, Debugging Programs On Win32, Nanomites And Misc Stuff, Full Reverse(Target: tElock), Full Reverse(Target: MrStop's Crackme #1), Full Reverse(Target: Inline patching nSPack 2.x), Xtream Exploiting Steps, Exploiting Non-Exec Stack, Exploiting Stack BOF Over SEH, Security Of Web Pages, How To Stay OUT Of JAIL, Secret Of BSOD, and Recent Computer Networks.
November 9, 2005	phzine04.zip	N/A	Phearless Serbian/Croatian Security Magazine Issue #04. Included in this issue: Symbian C++ Reference - Part 1, Symbian OS - Polymorphic MDL, TINY phile about SQL injections, Developing Network Security Tool(s), The Art of Reversing, Open Your Windows (OS), Malloc Demistified - Part 1, Bypass DEP on Heap, Client/Server Systems, Uncommon Tribute to Practical Switching, and Cisco Routers Exposed.
November 9, 2005	scapy-1.0.2.tar.gz	N/A	A powerful interactive packet manipulation tool, packet generator, network scanner, network discovery tool, and packet sniffer that provides classes to interactively create packets or sets of packets, manipulate them, send them over the wire,

			sniff other packets from the wire, match answers and replies, and more.
November 8, 2005	atutor_151pl2_xpl.php atutor151pl2.txt	No	Proof of Concept exploits for the ATutor SQL Injection vulnerability.
November 8, 2005	ibProArcade.txt	Yes	Exploit details for the ibProArcade Module SQL Injection vulnerability.
November 8, 2005	ipb.2.1.txt ipb.2.1-english.txt	No	Exploit details for the Invision Power Board Multiple Cross-Site Scripting & HTML Injection vulnerabilities.
November 8, 2005	phpWebThings144.txt	No	Exploit details for the phpWebThings Cross-Site Scripting & SQL Injection vulnerabilities.
November 8, 2005	prdelka-vs-BSD-pttrace.tar.gz	Yes	Exploit for the NetBSD pttrace() root vulnerability.
November 8, 2005	qbrute-v1.1.zip	N/A	A MD5 Calculator and Cracker written in Perl.
November 8, 2005	qcrack-v0.25.tgz	N/A	A program written to test the security of md5/md4/md2 passwords by attempting to brute force them.
November 8, 2005	susechfn.sh	Yes	Script that exploits the Multiple Vendors CHFN User Modification ROOT Access vulnerability.
November 8, 2005	tkadv2005-11-001.txt	Yes	Exploit details for the PHPList Multiple Input Validation vulnerabilities.
November 8, 2005	twiki20030201.pl.txt	Yes	Exploit for the TWiki Search Shell Metacharacter Remote Arbitrary Command Execution Vulnerability.
November 8, 2005	waraxe-2005-SA043.txt	Yes	Exploit details for the Phorum SQL Injection vulnerability.
November 8, 2005	x_dtsuids.pl.txt	Yes	Exploit for the Solaris 10 DtPrintinfo/Session vulnerability.
November 8, 2005	zone.labs-fw.txt	No	Proof of Concept exploit for the ZoneAlarm Personal Firewall Program Control Feature Bypass vulnerability.
November 7, 2005	fsigk_exp.py	Yes	Proof of Concept exploit for the F-Secure Anti-Virus Gatekeeper & Gateway for Linux Elevated Privileges vulnerability.
November 7, 2005	hpux_ftpd_preauth_list.pm	Yes	Proof of Concept exploit for the HP-UX FTP Server Directory Listing Vulnerability.
November 7, 2005	lnxFTPDssl_warez.c	No	Script that exploits the Linux-FTPD-SSL FTP Server Remote Buffer Overflow Vulnerability.
November 7, 2005	netmail.txt	No	Proof of Concept exploit for the Novell Netmail Script Insertion Vulnerability.
November 5, 2005	formatPaper.txt	N/A	A whitepaper that discusses further advances in the exploitation in format string bugs.
November 5, 2005	WifiScanner-1.0.1.tar.gz	N/A	An analyzer and detector of 802.11b stations and access points that can listen alternatively on all the 14 channels, write packet information in real time, search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.
November 5, 2005	wzdFTPd.pm.txt	No	Exploit for the Wzdftpd SITE Command Arbitrary Command Execution Vulnerability.
November 4, 2005	20051021.MS05-047.c	Yes	Remote Denial of Service exploit for the Microsoft Windows Plug and Play Arbitrary Code Execution vulnerability.
November 4, 2005	coarseknocking-0.0.2.tar.gz	N/A	A simple implementation of Port Knocking techniques that sniffs network packets looking for predetermined keys and executes commands to open and close ports on the firewall.
November 4, 2005	CuteNews1.4.1.txt	No	Exploit for the CutePHP CuteNews Directory Traversal & PHP Code Execution vulnerability.
November 4, 2005	galerie_2.4_exploit.pl gallery24.pl.txt	No	Proof of Concept exploits for the Gallery SQL Injection vulnerability.
November 4, 2005	gpsdrive-ex-long-ppc.pl gpsdrive-ex-short-x86.pl gpsdrive-ex-long-ppc.pl.txt	No	Proof of Concept exploits for the GpsDrive Remote Format String vulnerability.
November 4, 2005	phpinfoXSS.txt	No	Proof of Concept exploit for the PHP 'phpinfo.php' Cross-Site Scripting vulnerability.
November 4, 2005	qbrute.zip	N/A	A MD5 Calculator and Cracker that is written in Perl.
November 4, 2005	rna_deleter.rgp rna_bof.rgs	No	Scripts that exploit the RealArcade Vulnerabilities.
November 4, 2005	ssf.zip	N/A	A tool that exploits the various weakness in VoIP-Phones.
November 4, 2005	StackBasedOverflows-Windows-Part1.pdf	N/A	A document titled "Writing Stack Based Overflows on Windows - Part I: Basic Concepts."
November 4, 2005	StackBasedOverflows-Windows-Part2.pdf	N/A	A document titled "Writing Stack Based Overflows on Windows - Part II: Windows Assembly for writing Exploits."
November 3, 2005	asusvsbugs.zip	No	Proof of Concept exploit for the code for Asus Video Security Buffer Overflow & Directory Traversal vulnerabilities.

November 3, 2005	cirt-40-advisory.pdf	No	Exploitation details for the IpSwitch Whatsup Small Business 2004 Directory Traversal vulnerability.
November 3, 2005	NeroNet1202.txt	No	Exploitation details for the NeroNet Limited Directory Traversal Vulnerability.
November 3, 2005	php-handicapper.txt	No	Exploitation details for the PHP Handicapper Cross-Site Scripting & SQL Injection vulnerabilities.
November 3, 2005	scorchbugs.zip	No	Proof of Concept exploit for the Scorched 3D Multiple vulnerabilities.
November 3, 2005	up-imaproxy-exp.c	Yes	Proof of Concept exploit for the up-imaproxy Format String vulnerability.
November 2, 2005	bcarrydos.zip	No	Proof of Concept exploit for the Battle Carry Remote Denial of Service vulnerability.
November 2, 2005	flatfragz.zip	No	Proof of Concept exploit for the Johannes F. Kuhlmann FlatFrag Multiple Remote Buffer Overflow & Denial of Service vulnerabilities.
November 2, 2005	ggwbofc.zip ggwbof.zip	Yes	Proof of Concept exploits for the GraphOn GO-Global For Windows Remote Buffer Overflow vulnerability.
November 2, 2005	gliderbof.zip	No	Proof of Concept exploit for the Glider Collect'N Kill Remote Buffer Overflow vulnerability.
November 1, 2005	IEcrash.zip	No	Exploit for the Microsoft Internet Explorer Malformed HTML Parsing Denial of Service vulnerability.

[\[back to top\]](#)

Trends

- **Spyware Has Become A "Global Pandemic" For Enterprises: Survey:** A new study by Webroot Software found that 48% of enterprise PCs are infected with adware. They found that the average enterprise PC had 3.9 adware infections in the third quarter of this year, up from 3.6 in the previous quarter. Source: <http://www.networkingpipeline.com/showArticle.jhtml?articleID=173600626>
- **New Linux worm crawls the web:** A new Linux worm is crawling the web looking for a large number of vulnerable PHP systems and applications. The worm, known as Linux.Plupii (Symantec) or Linux/Lupper.worm (McAfee). It installs a Trojan using wget and the attack allows for arbitrary code execution under the privileges of the web server user. The worm exploits PHP based vulnerabilities discovered back in June, and affects a large number of PHP web applications that use XML-RPC. Source: <http://www.securityfocus.com/brief/38>.
- **US-CERT is currently aware of a new worm** which targets web servers running vulnerable versions of XML-RPC for PHP. Once the worm infects a web server, it opens a backdoor to the compromised server and begins scanning for additional servers to infect.
- **Phishing Alert: Google:** Websense® Security Labs™ has received reports of a new phishing attack that targets users of Google's search engine. Users are redirected to a spoofed copy of Google's front page with a large message claiming "You WON \$400.00 !!!". They are presented with instructions for collecting their prize money, which included entering credit card numbers and shipping addresses. Once the information has been collected, users are directed to Google's legitimate website. Source: <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=332>.
- **Online ID theft worsens, scares U.S. bank customers:** Banks and regulators have increased their efforts to stop identity theft over the Internet but many Americans fear that fraudsters remain one step ahead when banking online. Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,106066,00.html/>.
- **Hey Linux Users: No Software Is Impenetrable:** The vulnerability that affects a Windows network today is very likely to infect a Linux or Unix network connected to it. Companies that fail to secure their Linux networks may find rogue code spreading and infecting interconnected Windows networks. Source: http://www.newsfactor.com/story.xhtml?story_id=02000000GPIG.

[\[back to top\]](#)

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling anti virus, and modifying data.

3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
5	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
6	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
7	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
10	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.

Table updated November 7, 2005

[\[back to top\]](#)

Last updated November 10, 2005